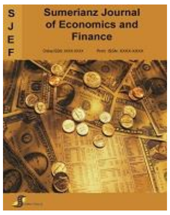
Sumerianz Journal of Economics and Finance, 2022, Vol. 5, No. 1, pp. 20-30
ISSN(e): 2617-6947, ISSN(p): 2617-7641
Website: https://www.sumerianz.com
DOI: https://doi.org/10.47752/sjef.51.20.30



Original Article Open Access

Detecting Fraudulent Billing Frauds Under The Shell Company Schemes: From the Perspective of Hong Kong Auditors

Dr. Benjamin Fung
Certified Fraud Examiner, Hong Kong
Email: bfung2012@gmail.com

(Corresponding author)

Article History

Received: 10 December 2021

Revised: 5 February 2022

Accepted: 8 February 2022

Published: 10 February 2022

How to Cite

Benjamin, F. (2022). Detecting fraudulent billing frauds under the shell company schemes: from the perspective of Hong Kong auditors. *Sumerianz Journal of Economics and Finance,* 5(1): 20-30.

Abstract

Asset misappropriation, which occurred in the vast majority of fraud schemes, involved stealing or misusing the company's assets and resources by perpetrators through false invoicing and shell company schemes. False invoicing occurred when a perpetrator created a fictitious vendor for purchasing goods for the employer, used false invoices to make a claim for payment and diverted the fund to its own account. The main purpose of this study is to detect fraudulent billing frauds under the shell company schemes which pose significant risk to the organizations. Shell company operations mainly involve 1) a perpetrator created a shell company, which was only a fictitious name with P.O. Box address, added it to the current vendor master file to facilitate the company's purchases and also used it to receive payment from false billings; and 2) the shell company was also used as an intermediary to assist the pass-through scheme wherein a legitimate vendor sold goods to this shell company which in turn resold goods to the victim organization with a certain percentage markup on price. Shell company and billing schemes did not receive much attention in prior audit literature and audit practices. This study aimed to investigate the level of effectiveness of red flags in detecting the fraudulent billing schemes from the perspective of auditors (inclusive both external and internal auditors) in Hong Kong and also to explore the effectiveness of fraud data analytics in detecting the billing schemes under the shell companies. For the assessment and perception of red flags for fraud detection, the study extracted a total of 15 red flags from Kassem's framework and used questionnaire survey to examine the auditors' responses to red flags in detecting fraudulent billings and release the resultant ranking. Sem-structured interviews were used to obtain data about the effective use of data analytics by auditors to detect fraudulent billings under the shells.

Keywords: Asset misappropriation; Fraudulent disbursements; Fraud risk indicators; Data mining and fraud; Data analytics.

1. Introduction

The introduction section explains the rationale for undertaking the study and describes the main purpose of conducting it. This study aims to address the literature gap on detecting asset misappropriation and explores the use of fraud data analytics to detect illegal shells. It also investigates whether firms interacting with shell companies would face a higher likelihood of being engaged in fraudulent activities. Data collection comprised online questionnaire and qualitative semi-structured interviews and the interviewees came from both internal and external auditors in Hong Kong. The conclusion presents the overall results of the study and discusses the effectiveness of fraud data analytics in detecting fraudulent billing schemes.

Every organization is at risk for fraud and fraudulent activities will go undetected for quite a while. A red flag is depicted as an observable event that auditors detect a fraudulent transaction. Red flags are generally important indicator of potential fraud. Internal auditors often observed red flags for early detection of frauds and also used them as the basis for determining the legitimate business transactions. During the process of fraud risk assessment, internal auditors attributed greater importance to red flags related to the business activities and internal control procedures of the company and perceived the relevance of red flags as the warning signs of the potential occurrence of billing fraud. Mangala and Kumari (2016) indicated that auditors had good perception of red flag as an effective tool to detect and prevent fraud.

Fraud has been a major concern for investors, regulators, and external auditors due to the widespread of notorious corporate frauds such as Société Generale, Enron, WorldCom, Adlephia., etc. As can be seen from the above cases, all frauds and collapse of large global corporations were greatly attributable to the fact that the prevalence of different types of fraud schemes and occurrence of fraudulent transactions could not be early detected by auditors thus causing losses to the companies.

In recent years, fraud prevention and fraud detection have gained a lot of attention, particularly, the shell company fraud scheme. Fraudsters are using shell companies to hide their illicit transactions and management have become increasingly concerned about the growing threat that adversely affects both businesses and customers. As usual, management would be most likely to write off the fraud losses and not investigate further to avoid wasting more money. This study was motivated that early investigation and detection might provide a better understanding of the fraud, help develop and implement fraud detection program to avoid the mistakes in the future.

2. Literature Review

There are many types of fraud taking place within the business world, and almost all occurrences result in financial losses for the organizations. This study placed emphasis on the billing schemes, one of the major fraudulent disbursement schemes of asset misappropriation. In a billing scheme, a dishonest employee commits fraud either by creating a shell company or by manipulating an existing vendor to make fictitious purchases to obtain personal benefit.

The literature review aimed to provide a comprehensive coverage of fraud detection themes as follows:

2.1. Asset Misappropriation

According to the Association of Certified Fraud Examiners (2010), occupational fraud is categorized into *asset misappropriation, financial statement fraud* and *corruption.* Asset misappropriation is reputed to be the most common and costly type of internal fraud committed by perpetrators who make a false claim to the employing company for payment. Perpetrators are usually able to disguise or conceal their fraud in ways that are not easy to detect.

According to Association of Certified Fraud Examiners (2020) Report to the Nations concerning Global Study on Occupational Fraud and Abuse (Global Fraud Study), asset misappropriation was the most common form and costly type of fraud accounting for 86% of the 2,504 fraud cases from 125 countries investigated in their study with the median loss at USD100,000 per case and the highest loss of USD954,000.

2.2. Billing Schemes

There are three sub-categories of asset misappropriation viz. *skimming schemes, cash larceny and fraudulent disbursement schemes* (ACFE, 2014). Billing scheme, one of the fraudulent disbursement schemes, could be committed by perpetrators through the creation of fictitious shell companies that issue fake invoices to the victim company for phantom products or services (Silverstone and Sheetz, 2007).

Billing schemes involved creating fake invoices for fictitious goods by perpetrators who inflated invoice amount for their personal gains. Instead of buying goods directly from a vendor, a scrupulous employee purchases the goods from the created shell company and then resells the goods to its employer at an inflated price. In this connection, vendors might even collude with perpetrator to help them pass through the company internal control system (Greene, 2003).

Association of Certified Fraud Examiners (2020) Global Fraud Study indicated that the median duration of a fraud (typical time counting from the beginning of a fraud to the time of detection) was 14 months. Reportedly, the maximum billing scheme could last for 24 months. The reason why the auditors took longer time to detect fraud was the time constraints of each audit assignment and the spending of resources on the audit process which might restrict the auditors' willingness to impose additional audit tests on emerging red flags.

2.3. Auxiliary Roles of Shell Companies

Shell companies are often established by individuals and businesses for the sole purpose of conducting legitimate transactions such as asset transfers, restructuring and corporate merger. On the other hand, shell companies are also created by the fraudsters as the corporate vehicle to commit a variety of fraud schemes, such as asset misappropriation, money laundering, bribery., etc. With the rapid increase in number of incorporated shell companies, the enforcement authorities are more concerned whether they would be used as corporate vehicles to commit fraud (Association of Certified Fraud Examiners, 2020). While not all engaged illegal business, shell companies have been received a lot of attention over the last few decades for their auxiliary roles in illegal activities and crimes. The incorporation of shell entities had been clearly shown in the growing corporate crimes in recent years due to the provision of a corporate veil to the fraudsters to remain anonymous (Association of Certified Fraud Examiners, 2020).

A shell corporation mainly plays an intermediary role in completing the business transaction without conducting any manufacturing nor commercial business (Nefsky, 1977). In billing schemes, shell companies might only be a fabricated name and address that were used by perpetrators to collect payments from false billings. In this context, shell companies could be used for receiving payments made to the order of the shell company name, perpetrators set up bank account in the shell name to receive and cash the fraudulent cheques. Thus, a shell company is only a fictitious entity which has been established exclusively to perpetrate a fraud. A shell company is usually anonymous hence it will be difficult to track the money going into and out of its accounts thus making it a good venue for perpetrators to commit fraud.

2.4. Red Flags: The Risk Indicators

Red flags are usually one of the key indicators of potential fraud. Auditors might observe a red flag that links to a fraudulent transaction during the audit process. A red flag exists in data, documents, internal controls, behavior, and public records. After establishing the red flags, internal auditors can begin an investigation into whether there are internal control weaknesses present in the operation system and whether these weaknesses are being exploited (Vona, 2019).

Kassem (2014) developed a specific framework for assisting external auditors in Egypt to properly assess and perceive red flags to detect material misstatements arising from asset misappropriation. According to Kassem, the list of red flags was derived from Wells (2005) textbook viz. *Principles of Fraud Examination* that covered a wide variety of US and many other countries' fraud cases. Although this framework was used to assess perceptions of external auditors in Egypt, it could still be applied and used by external auditors in any other country because the list of red flags was extracted from practical examples meeting fraud audit professional standards that are applied by different countries (Kassem, 2014).

There have been extensive researches in the use of red flags as an audit tool. Vicky *et al.* (1996), supported the use of red flags in helping auditors to facilitate their fraud risk assessment and detection. The research findings of Kassem and Hegazy (2010) indicated that the ranking of all red flags for fraudulent reporting according to their relative importance based on the external auditor opinions help focus their efforts more on high quality of red flags which would in turn facilitate their fraud detection. A pervasive view was held that the use of the 'red flags' had substantial predictive capabilities to detect fraud (Saksena, 2001; Summers, 1998) and Newman *et al.* (2001).

2.5. Perception of Importance of Red Flags by the Auditors

Red flags could provide auditors with crucial evidence about the possibility of fraud. Thus, both external and internal auditors are expected to know and perceive the importance and use of red flags in detecting fraud.

Gullkvist and Jokipii (2012) studied whether internal auditors, external auditors, and fraud investigators had different perceptions about the importance of red flags across asset misappropriation and fraudulent financial reporting. The results of G & J's research confirmed that there were significant differences in perceptions among the participant groups in which internal auditors reported a tendency of higher perception of importance of red flags relating to detecting asset misappropriation than those relating to fraudulent financial reporting. Conversely, external auditors reported equal perception of importance of red flags across asset misappropriation and fraudulent financial reporting. Based on other empirical research findings, there was no difference between external and internal auditors related to their overall perceptions of importance of red flags. However, the researchers recognized a difference in their respective role: internal auditors are generally company-hired employees and report directly to the board while external auditors are always appointed to perform audit assignment for their clients. Due to their role differences, internal auditors must be sensitive to all possible frauds and in response to red flags in fraud detection reflecting that they are loaded with internal control responsibilities and must have audit skills and experience to carry out the tasks. For the external auditors, they might be responsible more for fraudulent financial reporting than asset misappropriation.

All in all, red flags might have different weights related to fraud susceptibility. Assignment of weight to each red flag related to the possibility of a fraud occurred would be determined by the auditors' fraud training, fraud exposure and audit experience. Therefore, it is imperative for the auditors to understand and interpret each red flag related to the fraud scenario and reach conclusion about the occurrence of the fraud scenario.

2.6. How Data Analytics can Assist in Fraud Detection?

Fraud data analytics is the process applying data mining techniques to analyze data for red flags that related to a specific fraud scenario. The process begins with preparation of a fraud data analytics plan and also covers with the audit examination of documents, data records, internal controls, and interviews of employees to detect red flags in the transaction (Vona, 2019).

There is lesser literature on research into data analytics methods. In essence, fraud detection requires a unique and specific skill for detecting the critical evidence of fraud. According to Singleton *et al.* (2006) fraud detection requires well experienced individuals in using the applicable investigative and analytical tools to examine accounting records, gather and evaluate the relevant financial evidences and interview all parties related to an alleged fraud situation. For red flag detection, the auditor must collect all critical evidences on the company from many different sources and analytically examine all obtained data in order to determine the red flags in the most effective way (Ramos, 2003). Red flags could be categorized in the form of *data*, *documents*, *internal controls*, and *behavior* which might be very useful to facilitate the auditor's identification of red flags. For example, a vendor invoice number can be a data red flag or a document red flag observed through the examination of the vendor invoices.

Automation of fraud detection, which had become one of the prevalent business data mining applications, could help reduce the manual screening and checking process. Computer aided audit techniques (CAATs) used the computer as an audit tool for the application of auditing procedures (Braun and Davis, 2003). Early in 1982, CAATs were proven a powerful audit tool for detecting financial errors and misstatements. During the recent years, CAATs have been widely used by auditors to scrutinize large volumes of data, which it would be inefficient to do manually, and detect anomalies in financial records. Most importantly, auditors might make frequent use of fraud data analytics to detect anomalous or suspicious transactions. Since CAATs used computers as audit tool to automate or simplify the audit process, auditors might use *Microsoft Access* audit software to obtain a quick overview of the business operations and analyze individual transactions that contain salient features of fraudulent activities.

Data mining was a powerful tool to help find patterns and relationships within the data records as well as detect hidden information from large databases (Elkan, 2010). To enhance good understanding of these patterns, it is most important to look at two types of data: *relationships and transactional activity*. By taking an aggregation of both internal and external sources of data, one could detect series of connections between various entities and also gain a thorough understanding of their ownership structure, related affiliation and transactional flows. Since there should be a close link of every business transaction to both vendor master file data and transactional file data of purchase order, vendor invoices and payments, etc., one would search for the shell company established by a perpetrator in submitting fake invoices for selling fictitious goods to the victim organization. Through critical data pattern analysis, it would be easy for the auditors to detect the identity of suspicious vendors that might be the participant of a shell company scheme. Moreover, data mining could provide a wide range of techniques for detecting useful information from massive record data of trends, patterns and rules. These techniques employed the series of processes viz. data pre-processing, data analysis, and data interpretation in the course of data analysis (Adedoyin-Olowe *et al.*, 2014). However, there had been a short of data mining researches in fraud detection and the availability of publications of various well researched methods and techniques.

3. Methodology

This study looked at the level of awareness and perception of red flags by the auditors as an important tool for fraud detection in the audit process. Primary data were collected through online questionnaire survey about auditors' perception and semi-structured interviews about how auditors used fraud analytics to detect shell companies and the fraudulent billing schemes. Respondents joining the questionnaire survey were targeted to include both external and internal auditors in Hong Kong.

3.1. Methodological Framework

This study adopted the methodological framework to facilitate respondents to assess the relative importance of the designated red flags and then decide their ranking. Kassem (2014) conducted a questionnaire survey with the design of a framework for external auditors in Egypt for detecting a total of 52 red flags extracted from different categories of asset misappropriation. This study extracted only a total of 15 red flags from the billing schemes of the original Kassem's framework and revised the wording to suit the purpose of the questionnaire survey in Hong Kong.

3.2. Research Design

The research design of this study was shown in Table 3.1:

Table 3.1. Showed data collection methods, design format and nature of analysis of the study

Collection Methods	Design format	Nature of Analysis
Questionnaire	Perceived whether red flags were effective in detecting fraud.	Qualitative
	Ranked each of red flags according to their relative importance in detecting fraud.	Qualitative/ Quantitative
	Suggest using the relevant audit procedures in response to red flags for billing schemes.	Qualitative
Interviews	Categories of shell companies and various methods of detection.	Qualitative
	Data mining and fraud audit procedures.	
	Basics and effectiveness of data analytics.	

Contents of questionnaire were pilot tested by experienced internal and external auditors working in different local and international audit firms in Hong Kong and were revised as per the feedbacks received from the reviewers to rephrase some of the questions to make it easily understandable by the local audit respondents without making any change to the style of questions.

3.3. Data Collection Methods

In this study, online questionnaire was used to measure the respondent's perceptions of the relative importance of red flags for determining their ranking and also explore their suggested audit procedures to be used to detect billing frauds.

Online survey was the most widely used research methods to gather data from the respondents through the questionnaire over the internet in lieu of the traditional method of sending questionnaire by mail to respondents and the latter completed and sent them back by mail to the researcher. Questionnaire using google form is easy to use and offers greater convenience to respondents to complete questionnaire at their own pace thus boosting the response rate.

Semi-structured interviews were the second phase of data collection from the senior auditors/partners and forensic experts with a view to gaining an update on the fraud data analytics currently used by the auditors to detect billing frauds. Rubin and Rubin (2005) posited that semi-structured interview could provide the interviewer with the opportunity to probe and expand the interviewee's responses to gain in-depth information from the interviews.

4. Summary of Findings and Discussions

4.1. Questionnaire Findings

This section presented the overall results of the online questionnaire survey and demographics of the respondents. The contents of this questionnaire aimed to address the question of "*Do the auditors perceive red flags as an effective tool in detecting the possible frauds in billing schemes?"*

4.1.1. Demographics of Respondents

Online questionnaire survey had started since early 2021 and only received a total of 68 responses. Contents of this questionnaire contained certain highly complicated audit questions that required respondents to have extensive years of audit experience and fraud exposure. Table 4.1, 4.2 and 4.3 showed the percentage distribution of the online questionnaire survey (based on n= 68 responses) in terms of respondents' years of audit experience, role in audit firm and type of audit firm in Hong Kong and Table 4.4 the demographics of the respondents. Such information was critical to the study because if respondents lacked of fraud knowledge or audit experience, they might not want to join the questionnaire survey or deliberately make a guess at the answer, or provide a neutral mode of answers, which tended to reduce the reliability of data.

Table 4.1. Respondents' years of audit experience

(0-2) years	*(3-5) year)*	*(6-10) years*	*(11-15) years*	*Over 16 years of experience*
1.5%	7.4%	38.2%	33.8%	19.1%

Table 4.2. Type of Respondents' audit firm

Local	*International*	*Big 4**
41.2%	35.3%	23.5%

**Big 4 audit firms in Hong Kong include KMPG, Deloitte, PwC and Ernst & Young.*

Table 4.3. Respondents' role in audit firm

External Auditor	Internal Auditors
33.8%	66.2%

Table 4.4. Demographics on Respondents (External and Internal Auditors)

	None	Slightly	Moderately	Extensive	Extreme
What is your exposure to red flags?	7.4%	47.1%	39.7%	5.8%	-
	Never	Rarely	Occasional	Frequently	Always
How often do you use red flags?	4.4%	38.2%	50%	7.4%	-
	Yes	No			
Have you ever used red flags to detect fraud?	83.8%	16.2%			
	Yes	No			
Attended conferences on fraud detection using red flags?	80.9%	19.1%			
	Yes	No			
Has firm offered in-house red flag training?	85.3%	14.7%			
	<-10	11-15	16-20	21-25	>25
CPE hours on red flag and fraud detection?	11.8%	16.2%	47.1%	11.8%	13.1%
	Seldom	Somewhat	Mostly	Very	Extremely
How effective in firm in using red flags?	11.9%	46.3%	38.8%	3%	-
Position in firm	Partner	Director	Manager	Senior	Staff
	11.9%	10.5%	31.3%	28.4%	17.9%
Gender	Male	Female			

	41.2%	58.8%			

The demographics showed that all respondents were experienced in their role as either external or internal auditor. In this study, only 39.7% of respondents had moderate exposure to red flags and 5.8% extensive exposure to red flags. Only 50% of respondents occasionally used red flags and 7.4% frequently used red flags. Also, 83.8% of the respondents replied that they had ever used red flags to detect fraud. In a study by Pincus (1989), 50% of the respondents admitted to using red flags and only those who had hand-on fraud exposure considered red flags as a very useful tool in fraud detection.

4.1.2. Effectiveness of Red Flags in Fraud Detection

There were four sections in the questionnaire. Section A concerned response to a question of:

"Do you agree that each of the following red flags is effective in detecting fraudulent billing schemes?"

There was unanimous result that red flags would be effective predictors of fraudulent billing schemes within asset misappropriation. This result was consistent with previous research findings (Mock and Turner, 2005; Moyes, 2007) about external or internal auditors' perception of the important red flags related to fraud assessment.

4.1.3. Ranking of Relative Importance of Red Flags

Section B concerned the respondents' response to a question of:

"Do red flags have equal importance within billing schemes?"

Appendix 1 showed total frequencies of responses from the respondents about the 15 red flags. Table 4.5 presented the final ranking of 15 red flags for the billing schemes.

Table-4.5. Final Ranking of 15 red flags for the billing schemes

1	No separation of duties in the purchasing process - allowing a person who processes payments and approves new vendors.
2	Unexplained increases in the quantity of goods purchased.
3	Unfamiliar vendors or variations on an approved vendor's name
4	Purchases that cannot be traced to inventory.
5	An increase in cost of goods sold relative to sales.
6	Sudden increases in purchases from one vendor or payment to multiple vendors for same product.
7	Large billings are broken into multiple smaller invoices that will not attract attention.
8	Significant increases in average unit price of goods purchased could signal pass-through schemes.
9	Repeat billing for the same or similar amounts which are below the perpetrator's approval limit.
10	Vendor addresses match employee addresses.
11	Vendors only have a post office box address – could be a sign that they do not actually exist or a shell company.
12	Lack detailed descriptions of the items on the fraudulent invoices.
13	An increase in expenses from previous years.
14	*Unusually quick turnaround of invoices* meaning the fraudster is in a hurry to cash in.
15	Organization's expenses exceed budget projections.

4.1.4. Summary of Audit Procedures of Red Flags

Among the 15 ranked red flags, the majority of the items can be judged important due to the prima facie evidence like no separation of duties in the purchasing process. However, there was a total of seven items (Nos. 2, 5, 9, 11, 12, 13, and 15) that required the respondents to use analytical procedures, examine ledgers and journal entries, stock counting, and inquire management, employees and vendors about emergence of red flags in the billing schemes. Section C of the questionnaire accommodated the request for information on likely audit procedures of the red flags in question from the respondents.

Table-4.6. Summary of likely audit procedures of the ranked red flags Nos. 2, 5, 9, 11, 12, 13, and 15, to be used by the respondents

Red flags	*Audit procedures*
Unexplained increases in the quantity of goods purchased. (No. 2)	Check the procurement policy and ask the purchasing manager to provide a report explaining the reasons for such increase.
An increase in cost of goods sold relative to sales. (No. 5)	Analytical procedures of reviewing addition of purchases, overall stock sold and the closing stock balance.
Repeat billing for the same or similar amounts which are below the perpetrator's approval limit. (No. 9)	Sort payments by vendor and amounts. Ask the purchasing manager for explanation about this phenomenon.
Vendors only have a post office box address – could be a sign that they do not actually exist	Check the sales records whether this questionable vendor is an old or a new vendor. Verify its

or a shell company. (No. 11)	physical existence by site visit and telephone. If failed, report the matter to management to take the required action.
Lack detailed descriptions of the items on the fraudulent invoices. (No. 12)	Inquire management about the matter and ask for a duplicate invoice to show the descriptions, quantity, terms, unit price and the total amount billed.
An increase in expenses from previous years. (No. 13)	Conduct horizonal analysis of the expenses on a yearly basis and analyze the trend patterns.
Organization's expenses exceed budget projections. (No. 15)	Compare between actual and budgeted expenses to find out the difference and investigate the reasons for large difference.

4.2. Interviews Findings

The primary purpose of the four semi-structured interviews was to gain a thorough grasp of the problems of shell companies in the billing schemes. These interviews aimed to answer the following two research questions:

1. *How might the auditors use the fraud data analytics to identify shell companies?*
2. *Are the fraud data analytics effective method to detect the fraudulent billing schemes?*

Three external auditors and one internal auditor were invited to attend the interviews during the period of February and March 2021, each of the interviews lasted between one hour and one and a half hours. Table 4.7 showed demographics of the four interviewees as follows:

Table 4.7. Demographics on Interviewees

Interviewee	Position	Type of Auditor	Type of Audit Office	Years of Audit Experience	Exposure to Red Flags
Interviewee 1	Partner	External	Big 4	➢ 20	Yes
Interviewee 2	Director	External	International	➢ 20	Yes
Interviewee 3	Principal/ Forensic Consultant	External	Local	➢ 25	Yes
Interviewee 4	Senior Manager	Internal	Local	➢ 15	Yes

The following subsections focused on the discussions about the formation of different categories of shell companies and their functions; the exploration of the power of data mining and fraud audit procedures; and the commentary on the effectiveness of the relevant billing fraud detection methods.

4.2.1. Categories of Shell Companies

All interviewees unanimously indicated that a shell company might play a critical role in the billing transactions and emphasized that the shell company was not necessarily illegal, but dishonest employees can use them as a transactional vehicle to commit billing fraud. In many instances, perpetrators would not just form one shell company but might need to form a number of different shell companies to conceal a fraud. Based on their expertise in fraud and audit experience, they indicated that there were five primary categories of shell companies for billing schemes as follows:

1. Created shell company
2. Assumed shell company
3. Hidden shell company
4. Conflict-of-interest shell company
5. Temporary shell company

They claimed that it would be very hard to spot the suspected shell company without getting any information about the rationale for shell company formation. Apart from greater scrutiny of ownership, they considered understanding of the important patterns of transactional activities and relationship would provide greater insight into *potential* shell companies.

They stated that unscrupulous employees established a shell company under the '*created'* shell company category and perpetrated a false-billing scheme to sell products to default the employing organization. They might add the name of this created shell company as the authorized vendor and also add it to account payable file to settle the purchases.

In an *'assumed'* shell company scheme, a perpetrator made use of a dormant existing vendor or outside legitimate vendor who was not yet included on the vendor master file to sell products to the victim organization. In a '*hidden'* shell company scheme, a real vendor operated under its own name for ordinary businesses and also used other different names to engage shell company sales. Further, there was a *'conflict-of-interest'* shell company, in which a perpetrator acting alone or in collusion with another staff that might form a shell company to become a sole client to their employing company. Lastly, a perpetrator might use a '*temporary*' shell company that might exist as name or paper company only for a limited number of transactions but would be dissolved later.

4.2.2. Why Shells Matter?

As previously mentioned, shell companies were nominees that had disguised their ownership in order to facilitate perpetrators to commit fraud without scrutiny from management. The interviewees also indicated that the use of shell company to perpetrate billing frauds had been common and the frauds became almost undetectable for a long time. In essence, shell companies were not illegal by themselves, however, the interviewees considered that shell companies and fraud were most likely related since perpetrators could utilize them as company veil to default their employing organizations. Accordingly, such phenomenon was greatly attributable to the existence of no strict separation of duties in which the perpetrators could make use of the formed shell companies as the transactional vehicles to make purchases and approve payment to their own selves.

4.2.3. Cracking the Shells

Perpetrators established anonymous shell companies to hide illicit transactions. The interviewees asserted that in most cases, shell companies were not easily detected by specific detective measures, but rather revealed through series of both external or internal due diligence mechanisms as follows:

1. Conduct company searches and web intelligence to detect the hidden identities of the true owners of the entities or the contact person of the shell companies;
2. Perpetrators' concealment strategy;
3. Analyzing master file and transactional file data when looking at shell company scheme; and
4. Whistleblower programs offered by the company to encourage staff to use hotlines to report the fraud incidents and evidence of the shell companies, either anonymously or using real name.

Auditors can conduct company particulars search, directors index search and other searches to obtain the required information on shell companies. However, perpetrators use nominees, and other shell companies as the registered owner of the established shell company. Some nominees were local accounting or company secretarial firms which were responsible for updating company records, signing the company documents, and forwarding mails. Shell companies might have website to provide information about the ownership, physical address and contact person details. Thus, auditors might require to track and trace the linkage of information with the employees and other entities to detect the operations of shell company schemes.

On the other hand, perpetrators would be very sophisticated to hide illicit transactions under the shell companies and there were low, medium and high level of sophistication of concealment. Auditors considered these three levels of sophistication for created vendor addresses for shell companies by matching a vendor's address with employee's address. Low sophistication happened when a direct match between a perpetrator's known address and the shell company address. This would be very easy for auditors to detect such a shell company. A close match between a perpetrator's known address and the shell company address (such as the close proximity in the same street and district) implied a medium sophistication. Finally, no match existed between the perpetrator's known address and the shell company address showed a very high sophistication of perpetrator.

4.2.4. Data Mining and Fraud Audit Procedures

Due to the momentum of shell company in the billing schemes, the interviewees shared their experience in using data mining techniques and fraud audit procedures to detect the fraudulent billing schemes.

A. Detection of Shell Companies

Most auditors often adopted the following approaches to detecting the creation of shell companies by perpetrators:

1. Compliance with incorporation requirements of Hong Kong limited companies with the stipulated provisions of share capital, names of shareholders and directors, company secretary, registered office address and contact information of designated representative.
2. Business capacity to trade with a critical review on the issued and paid-up capital of the entity as well as its gearing ratio.
3. Market intelligence about the business operations and comments of the entities.

The first step was to ascertain whether the entity was legally incorporated with full disclosure of the requisite company information. The next step was to verify an entity's physical existence by visiting its registered office address or making telephone contact with its principal officers. The applicable business capacity test was to verify whether the company could have the capacity to trade by virtue of its financial strength. For instance, a merchandising company, which bought good from the producers and resold to the customers, had a small paid-up capital of HK$100,000 and reported annual sales of HK$500 million. Given a small minimal equity base, this company incurred HK$400 million total liabilities including trade payable, and other accruals for its business. This company should be unable to obtain trade credit from the producers due to its high gearing of 40 times. Further, market intelligence was good tool to check about the reputation of the company. If a vendor was only used as a nominee company in the billing scheme for recording phantom sales and non-existent goods deliverable, there was no market commentary and reference checking from other vendors. Proof of transaction data like shipping documents, vendor invoices and reference checking from counterparts were required to verify an entity's business capacity.

On the other hand, external auditors would perform the task of examining the documents about sorting payment amount by vendor, complete descriptions of goods on invoice and invoice number to detect the red flags. Likewise, internal auditors would require to perform these requisite tasks during the course of internal audit.

B. Examination of Current Vendor Master Files

Auditors often performed audit procedures to pierce the concealment strategy of the company in order to uncover the shell company. The interviewees indicated that the use of data mining techniques, a process of searching, classifying, matching and retrieving data from transaction records, to compare current vendor master file to that of the prior year's file to see any marked discrepancies that should be investigated due to the possible fraud.

In light of the certain changes to data field items, the interviewees indicated that once any unusual transactions have been identified in some inactive vendors, immediate comparisons can be made to the account payable table for the same year regarding the amounts and frequency of payments made to any doubtful vendors in question.

All Interviewees indicated that a review of vendor master files can be manual or automated. For a smaller company, manual reviews of vendor master files may be sufficient. However, manually reviewing and comparing vast vendor master files in larger organizations can be tedious and time-consuming. Thus, *Microsoft Access* can be a useful tool in tracing the false billings as compared to other traditional audit procedures, like inspection of source documents, to find out the nature of the transactions. Moreover, *Microsoft Access* can provide management or the auditors with, for example, a detailed list of questionable transactions, employees and vendors which need further investigation.

4.2.5. Basics of Fraud Data Analytics

When searching for shell companies, auditors might focus on the key transactional data, such as purchase orders, invoices and payments to vendors. In essence, auditors might check whether purchase orders contain all the details of goods ordered; match between invoices and purchase orders; uninterrupted sequential invoice numbers; and legitimate vendor in the current vendor master file.

A. Invoice Number Patterns, Amount and Frequency

An invoice number was unique assigned to each invoice for easy identification for payment and audit. Perpetrators might conspire with venders to make phantom purchases and forge invoices and other supporting documents to complete the transaction. Thus, key transactional data like invoice and invoice number could signal document red flags through the examination of the vendor invoices. The most common practices on numbering invoices were sequential**,** chronological**,** customer name/number, or product number. Vendors provided an invoice number when they submitted an invoice for payment, and as a result the system should reject payments relating to invoices entered without invoice numbers. A general rule of thumb in accounting and best practices was to keep the invoice number in order without cancellation, recurring, gaps and skips. However, when an error occurred, vendor would create a new invoice and send to customer along with a note of correction.

More importantly, auditors might search for the patterns of the vendor invoice number and frequency to look for the evidence that was associated with the fraud schemes. Perpetrators might create invoice numbers with any letters or codes as they like. For instance, a sequential pattern or low starting invoice number such as INV-0001 might be a good indicator of a created shell company or conflict-of-interest shell company for the sole purpose of their unique identification. Hence, vendor submitted sequentially numbered invoices such as "INV-0001," "INV-0002," "INV-0003." to the company for payment. However, if the pattern of low starting invoice numbers continued to exist for a long while, this might adversely affect the sustainability of vendor as it only operated a single client business. When asked about the limited range pattern or illogical invoice number range, the interviewees indicated that a sophisticated perpetrator might intercept or withhold vendor invoice for the fictitious goods in order to conceal fraud. In this context, a vendor doing business with only one client might be fictitious.

Perpetrators might make use of their positional authority to approve payment of invoice amount within a predetermined control threshold in order to avoid scrutiny. If all invoice payments to a specific vendor were often below a key control threshold and well within perpetrator's approval limit, auditors might need to check whether this vendor worked as a shell company. For internal control purpose, internal auditor might check the payment history of vendors with details of invoice amount and payment frequency to look at the evidence of shell company.

B. Significance of Invoice Dates

Invoice date had the essential information for payment which was usually the date when the goods were sent to the buyer and billed the purchaser. Internal auditors might look at the evidence of an illogical order of transactions – set up invoice dates before purchase order dates – or unusual fast payment. Internal auditors might also check actual payment date to ascertain whether a perpetrator still made fast payment to vendor before the expiry of credit period. These anomalies might indicate the possibility of invoice fraud committed by both perpetrator and fictitious vendor.

4.2.6. Effectiveness of Fraud Data Analytics

This subsection summarized the overall discussions on the effectiveness of the relevant data analytics by all interviewees. In short, all interviewees unanimously agreed that fraud data analytics were essential to detect and prevent billing frauds, for instance, the analytical procedures like the matching of vendor master files to employee files to spot similarities for practicing pass-through scheme through shell companies and critical examination of invoice documentation are effective in detecting fraudulent billing schemes. There was no question that billing schemes had become more sophisticated, perpetrators were constantly finding ways to manipulate and conceal the frauds. With the advent of the updated audit methodology, sophisticated perpetrators might continue to seek better tricks to hide their illicit transactions accordingly.

The interviewees agreed that there were shortcomings with many controls testing methods like sampling. Auditors could not verify every single transaction due to time constraints and must rely on using sampling, however, sampling might miss many smaller anomalies which could result in very large frauds over time.

A. Why do Auditors Fail to Detect Fraud?

All interviewees unanimously agreed that many internal control systems had inherent weaknesses, the fraud data analytics might be somewhat useful and applicable to help detect the company's billing frauds. With the update on audit regulations and guidance as well as auditors' expertise and extensive audit experience, perpetrators might still be able to commit fraud without detection by auditors. Thus, auditor might continue to face with difficulties to track frauds and that could be the reason why frauds had been least detected by auditors.

In an extensive literature review, Hux (2017) found that auditors failed to recognize the need of using forensic experts to detect the frauds. Hux indicated that such phenomenon was attributable to auditors' overconfidence in their own abilities to detect frauds or failure to recognize the forensic expert's expertise in fraud detection.

B. Reasons for Fraud Without Detection

Association of Certified Fraud Examiners (2020) Global Fraud Study reported the median duration of a fraud occurred without detection was 14 months and billing scheme extended to 24 months. Despite the availability of increasingly sophisticated fraud detection techniques, there have been concern whether internal auditors could be able to shorten the duration of fraud occurred without detection.

Conceivably, management or supervisor might be the perpetrators to utilize their authority to instruct their subordinates to perpetrate the billing fraud by overriding of internal controls for the creation of a phantom purchase order and approval of a fake invoice for payment of fictitious goods. They would take steps to withhold information and falsify documentation to conceal the fraud from both internal or external auditors.

As a company employee, internal auditor might be difficult to detect management or supervisor for perpetrating fraud due to their override of ineffective internal controls. Further, there was also threat of management' outsourcing of some or all of the internal audit functions to an independent third-party firm thus ruining their career.

In short, data mining and fraud analytics were proven to be effective in reducing fraud loss and duration. However, these techniques were more applicable to larger organizations due to the practical need of huge investment in time and resources. Nevertheless, the interviewees remarked that existence of organizational culture with a high potential of fraud; unwillingness of employees to express their concerns; inadequacy of the whistleblowing procedures; and lack of monitoring disclosures are the major inhibiting factors for causing fraud without detection.

5. Conclusion

The use of red flags as an audit tool has been researched extensively. However, the number of prior research studies examining the perceived effectiveness of red flags for fraudulent billing schemes had been limited. This study investigated the level of effectiveness of the red flags for detection of the fraudulent billing schemes from the perspective of external and internal auditors in Hong Kong and offered to explore the role of shell company and the current state of fraud data analytics for billing schemes. This study also offered useful enlightenment to fraud data analytics for detecting red flags that related to billing fraud scenario. Hence, data analytics involved critical examination of transactional documents, review of internal control threshold, and inquiry of employees to detect the evidence of red flags or errors and the need for further investigation. All four interviewees, who were well equipped with good expertise in fraud and audit experience, provided with the most current and comprehensive fraud data detection methodology with good illustrations of practical examples in fraud audit process. This study also presented an integrative approach to look at the reasons for auditors' failing effort to detect billing fraud.

References

ACFE (2014). Report to the nations on occupational fraud and abuse 2014 Global Fraud Study.

Adedoyin-Olowe, M., Gaber, M. and Stahl, F. (2014). A survey of data mining techniques for social network analysis. *Journal of Data Mining and Digital Humanities*: Available: http://centaur.reading.ac.uk/40754/

Association of Certified Fraud Examiners (2010). Report to the nation on occupational fraud.

Association of Certified Fraud Examiners (2020). Report to the nation on occupational fraud.

Braun, R. and Davis, H. (2003). Computer-assisted audit tools and techniques: Analysis and perspectives. *Managerial Auditing Journal*, 18(9): 72.

Elkan, C., 2010. "Preserving privacy in data mining via importance weighting." In *Conference: Privacy and Security Issues in Data Mining and Machine Learning - International ECML/PKDD Workshop.*

Greene, C. (2003). Audit those vendors. *The White Paper*: Available: http://wps.prenhall.com/bp_revsine_finreport_3/22/5874/1503905.cw/content/index.htm

Gullkvist, B. and Jokipii, A. (2012). Perceived importance of red flags across fraud types. *Critical Perspectives on Accounting*, 1(3): 1–18. Available: http://www.elsevier.comGullkvist

Hux, C. (2017). Use of specialists on audit engagements: A research synthesis and directions for future research. *Journal of Accounting Literature*, 39(C): 23–51.

Kassem, R. (2014). Detecting asset misappropriation: A framework for external auditors. *International Journal of Accounting, Auditing and Performance Evaluation,* 1(10): 1-42.

Kassem, R. and Hegazy, M. (2010). Fraudulent financial reporting: Do red flags really help? *International Journal of Academic Research: Economics and Engineering,* 4: Available: https://ssrn.com/abstract=2011332

Mangala and Kumari (2016). Auditors' perceptions of the effectiveness of fraud prevention and detection methods. Available: https://journals.sagepub.com/doi/10.1177/0974686217738683

Mock, T. and Turner, J. (2005). Auditor identification of fraud risk factors and their impact on audit programs. *International Journal of Auditing,* 9(1): 59–77.

Moyes, G. (2007). The differences in perceived level of fraud-detecting effectiveness of SAS no. 99 red flags between external and internal auditors. *Journal of Business and Economics Research,* 5(6): 9-25.

Nefsky, R. (1977). federal income taxation and real estate development: Death knell for shell corporations? *Nebraska Law Review,* 56(3): 659-75.

Newman, D., Patterson, E. and Smith, R. (2001). The influence of potentially fraudulent reports on audit risk assessment and planning. *The Accounting Review,* 76(1): 59-80.

Pincus, K. (1989). The efficacy of a red flags questionnaire for assessing the possibility of fraud. *Accounting, Organizations and Society,* 14(1-2): 153-64.

Ramos, M. (2003). Auditors' responsibility for fraud detection. *Journal Of Accountancy,* 95(1): 28-36.

Rubin, H. and Rubin, I. (2005). *Qualitative interviewing: The art of hearing data.* Sage: Thousand Oaks.

Saksena, P. (2001). The relationship between environmental factors and management fraud: an empirical analysis. *International Journal of Commerce and Management,* 11(1): 120-43.

Silverstone, H. and Sheetz, M. (2007). *Forensic accounting and fraud investigation for non–experts.* 2nd ed. edn: John Wiley and Sons, Inc.: Hoboken, New Jersey.

Singleton, T., Singleton, J., Bologna, G. and Lindquist, R. (2006). *Fraud auditing and forensic accounting.* 3rd ed. edn: John Wiley and Sons, Inc.: Hoboken, NJ.

Summers, S. (1998). Fraudulent misstated financial statements and insider trading: An empirical analysis. *Accounting Review,* 73(1): 131-46.

Vicky, B., Hoffman, H., Morgan, K. and Patton, J. (1996). The warning signs of fraudulent financial reporting. *Journal of Accountancy,* 182(4): 75-77.

Vona, L. (2019). *Using data analytics to find fraud under those shells.* Fraud Magazine. 19-22.

Wells, J. (2005). *Principles of fraud examination.* John Wiley and Sons: Hoboken, New York.

Appendix 1

Total Frequencies of Respondents' response to the relative importance of the Red Flags in Questionnaire Survey

Red flags for billing schemes	1	2	3	4	5
● Unexplained increases in the quantity of goods purchased.	39				
● An increase in cost of goods sold relative to sales.	35				
● An increase in expenses from previous years.		17			
● Organization's expenses exceed budget projections.		11			
● Lack detailed descriptions of the items on the fraudulent invoices		25			
● Purchases that cannot be traced to inventory.	37				
● Significant increases in average unit price of goods purchased could signal pass-through schemes.	26				
● Vendor addresses match employee addresses.	21				
● Unfamiliar vendors or variations on an approved vendor's name.	37				
● Vendors only have a post office box address – could be a sign that they do not actually exist or a shell company.		29			
● No separation of duties in the purchasing process - allowing a person who processes payments and approves new vendors.	41				
● Large billings are broken into multiple smaller invoices that will not attract attention.	32				
● Repeat billing for the same or similar amounts which are below the perpetrator's approval limit.	24				
● *Unusually quick turnaround of invoices* meaning the fraudster is in a hurry to cash in.		14			
● Sudden increases in purchases from one vendor or payment to multiple vendors for same product.	33				