# Detecting asset misappropriation: a framework for external auditors

Rasha Kassem

The University of Northampton,
Boughton Green Road, Northampton, NN2 7AL, UK
E-mail: Rasha.kassem@northampton.ac.uk

**Abstract:** Fraud is a major concern for investors, regulators, and external auditors. Of particular concern is asset misappropriation because it was given less attention in prior audit literature as well as the audit practice though it is the most common type of occupational fraud. This motivated the current study to examine areas related to asset misappropriation that had never been examined before and alert external auditors in Egypt to a type of fraud which was given less attention. The current study also proposed a framework for external auditors that might help them properly assess and respond to fraud risk factors arising from asset misappropriation. This framework was designed after careful consideration of prior audit literature, Egyptian auditors' perceptions of the most important red flags of asset misappropriation, and their experience on the most effective fraud risk response. Study data was gathered using prior literature, a questionnaire, and a semi-structured interview.

**Keywords:** fraud; occupational fraud; asset misappropriation; red flags; fraud detection techniques; external auditors; auditor reputation; audit procedures; audit quality; audit expectation gap; audit risk.

**Reference** to this paper should be made as follows: Kassem, R. (2014) 'Detecting asset misappropriation: a framework for external auditors', *Int. J. Accounting, Auditing and Performance Evaluation*, Vol. 10, No. 1, pp.1–42.

**Biographical notes:** Rasha Kassem is currently a Lecturer in Accounting at the University of Northampton, Northampton Business School, UK. She is also a doctoral candidate at Loughborough University, Business School. In 2012, she was elected as a Training Director at the Certified Fraud Examiners (CFE) Chapter in Egypt. She is an active member of the European Accounting Association, the European Institute for Advanced Studies in Management (EIASM), the American Institute of Certified Public Accountants (AICPA), the Association of Certified Fraud Examiners (ACFE), the British Accounting and Finance Association (BAFA), and the American Accounting Association (AAA).

## 1 Introduction

Needless to say how costly fraud could be to any organisation. In fact, fraud cost is far beyond just financial losses because it can also result in high turnover, loss of productivity, increased fear of insecurity, and loss of confidence in the capital market and

audit profession. This makes fraud a major concern for investors, regulators, and external auditors.

There are many classifications for fraud but the current study and most prior literature broadly classifies fraud as either external fraud or internal fraud. External fraud is committed by individuals outside the organisation such as credit card fraud, investment fraud, customer's fraud, and vendor's fraud. In contrast, internal fraud is committed by employees of the company and is commonly known as either 'occupational fraud' or 'corporate fraud' (Johnson and Rudesill, 2001; O'Gara, 2004; Alleyne and Howard, 2005; Wells, 2005). Occupational fraud was defined by the Association of Certified Fraud Examiners [ACFE, (2002), p.4] as: "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organisation's resources or assets". Examples and categories of internal fraud include asset misappropriation, financial reporting fraud, and corruption (Wells, 1995).

The current study is more concerned about internal or occupational fraud, and more specifically asset misappropriation for several reasons. First, occupational fraud is the most common and costly type of fraud and occurs more frequently than external fraud (ACFE, 2010, 2012; PWC, 2010; Hassink, et al., 2010; Wells, 2005). Second, although asset misappropriation is the most common type of occupational fraud (ACFE, 2010), it was given the least attention in prior literature and no attention in Egypt. In addition, none of these few studies mentioned how external auditors could detect asset misappropriation or how they could properly respond to fraud risk factors arising from asset misappropriation. Third, although current professional audit standards [International Standards on Auditing No. 240 (ISA No. 240): "the auditor's responsibilities relating to fraud in an audit of financial statements"] expanded external auditors' responsibility for fraud detection, critics (Pedneault, 2004; Smith and Baharuddin, 2005; Zimbelman, 1997; Glover et al., 2003; Zikmund, 2008; Brazel et al., 2010; Mcdonald and Banks, 1997; Hogan et al., 2008; Srivastava et al., 2009; Shelton et al., 2001) argued that the standard provides little guidance to external auditors on fraud risk response with respect to asset misappropriation and financial reporting fraud. They also argued that ISA No. 240 did not assign weights for red flags, making external auditors assume that fraud risk factors are equally important. This could lead to an inefficient, ineffective, and inconsistent application of fraud risk assessment and fraud risk response.

The case of Egypt was of particular interest to the current study due to the scarcity of research about fraud in general and the lack of research studies into asset misappropriation in particular in the Egyptian context. Dahawy et al. (2010), and Hassan and Power (2009) argued that Egypt is characterised by the secrecy culture and management tend to view information as a private asset owned by the firm. This indicates that fraud news is less likely to be publicly available given the secretive culture that characterises Egypt. In the meantime, external auditors in Egypt are required to follow ISA No. 240. However, there is no evidence that this standard is actually implemented in Egypt, to what extent external auditors in Egypt are aware of fraud risk factors, and how they are more likely to respond to fraud risks arising from fraud. This motivated the current study to expand researchers and external auditors' knowledge about a type of occupational fraud that has been rarely investigated and to examine areas related to asset misappropriation (fraud risk assessment and fraud risk response) which have never been examined before in prior literature and the Egyptian context. The current study also provides external auditors with a framework that might help them properly assess and respond to risk factors arising from asset misappropriation. Although this framework was

based on perceptions of external auditors in Egypt, it can still be used by external auditors in any other country because the list of red flags proposed by the current study was derived from examples of fraud risk factors provided by audit professional standards (SAS No.99, ISA No. 240), and Wells 2005 textbook *Principles of Fraud Examination* which was based on real fraud cases that took place in different countries. Thus, the current study contributes to both knowledge and practice. To achieve the study's aims, mixed research methods were used (questionnaire and a semi-structured interview) to collect data from the study sample (external auditors in Egypt).

The rest of this paper is organised as follows: Section 2 defines, explains, and illustrates the different categories of asset misappropriation, and how each can be committed and concealed. Section 3 critically reviews prior research studies into asset misappropriation, highlights the gaps in the literature and presents the research main questions. Section 4 describes the methods used for data collection. Section 5 shows the main findings and data analysis. Section 6 presents and explains the proposed framework for detecting asset misappropriation. Section 7 draws the conclusion and provides insights for future research.

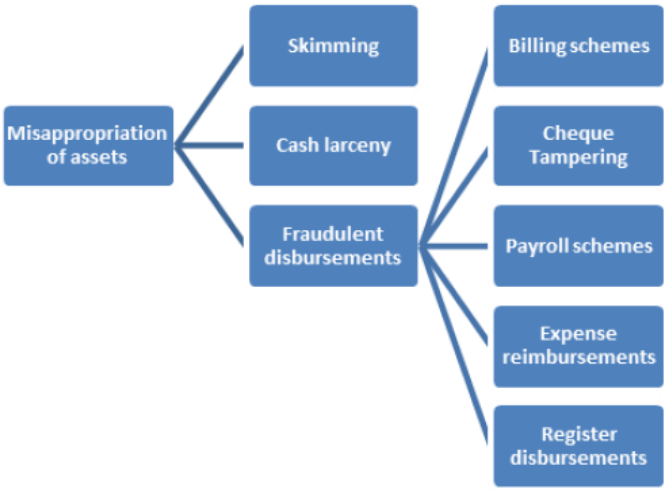
## 2 The nature and categories of asset misappropriation

Asset misappropriation involves stealing an asset of a company for personal use at the company's expense or misuse of a company's resources. Asset misappropriation is often accompanied by false or misleading records or documents to conceal the theft (Johnson and Rudesill, 2001; Wells, 2005; KPMG, 2006, 2007; Soltani, 2007; Lasko, 2009; Bayley and Eliff, 2009; ACFE, 2010). Thus, the definition of asset misappropriation is broader than simple theft as it also includes abuse of assets (Majid et al., 2010). Asset misappropriation is usually perpetrated by employees in relatively small and immaterial amounts. However, it can also involve management, who are usually more able to disguise or conceal misappropriations in ways that are difficult to detect (Soltani, 2007; Elder et al., 2010; Jones, 2011). According to ACFE (2010, 2012), asset misappropriation is the most common form of fraud representing 90% of the fraud cases investigated in their study. However, it was the least costly type of fraud, causing a median loss of $135,000. The ACFE study in 2010 was a global fraud study that involves many countries across the globe including Egypt, though there were only five fraud cases reported in Egypt. However, in the ACFE 2012 report, no fraud cases were reported from Egypt. This might again be justified by the secrecy culture in a developing country like Egypt where fraud news and fraud research are less likely to be publicly available. This further motivated the current study to explore a type of fraud that has never been researched before in the Egyptian context. Consistently, KPMG (2006, 2007) and PWC (2011) found that asset misappropriation is the most common type of occupational fraud.

In a study conducted by Wells in 1995, where he examined 2,608 cases of actual fraud provided by Certified Fraud Examiners, many of which occurred in the UK, results revealed that occupational fraud is classified into three main categories (asset misappropriation, financial reporting fraud, and corruption) and each of these categories is classified into further sub-categories, regardless of the international borders. Asset misappropriation was thus classified into three further sub-categories: skimming schemes, cash larceny, and fraudulent disbursements schemes. Figure 1 illustrates the

different sub-categories of asset misappropriation. This classification is commonly used by many practitioners and researchers as well such as the ACFE in its Reports to the Nation on Occupational Fraud and Abuse which was published in 2002, 2004, 2006, 2008, 2010 and recently 2012, KPMG in a study about occupational fraud in New Zealand in 2006 and 2007 in the Middle East region, and PricewaterhouseCoopers (PWC) in a study conducted in 2011 into asset misappropriation.

**Figure 1** Categories of asset misappropriation (see online version for colours)




*Source:* ACFE (2010, p.1)

As shown in Figure 1, the first sub-category of asset misappropriation is called 'skimming'. This type is very difficult to detect, investigate, and proof because it takes place before money is recorded in a company's accounting system leaving no audit trail. That is why it is called an off-book scheme. Skimming can be committed in numerous ways and detecting and preventing them varies from industry to industry. However, regardless of the industry, it is important to develop surprise audit procedures that would detect a skimming scheme (ACFE, 2010). Coenen (2009) argued that since skimming is so difficult to detect and prove companies should rely heavily on preventive controls that would make employees reluctant to steal. According to the ACFE 2010 report, skimming caused a median loss of $60,000 and the percentage of skimming cases account for about 14.5% of all reported fraud cases worldwide. The report also showed that skimming schemes are more prevalent in small sized organisations (with less than 100 employees) and was found to be prevalent in banking/financial services sectors followed by healthcare, public administration and manufacturing sectors.

Skimming happens at the point of entry of money into a business, and usually occurs in small, cash intensive business. Typical jobs that might involve access to funds in this way include bank teller, waitress, store cashier, salesperson, or medical billing clerk (Zweighaft, 2004; Wells, 2005; Silverstone and Sheetz, 2007; Hopwood et al., 2008; Coenen, 2009; ACFE, 2010). There are two types of skimming schemes:

1 sales skimming

2 receivables skimming.

*Sales skimming* are especially common when the fraudster has access to incoming funds from an unusual source, such as refunds that have not been accounted for by the victim organisation. While, *receivables skimming* are more difficult to conceal than sales skimming because incoming receivables payments are expected, so the victim organisation is likely to notice if these payments are not received and entered into the accounting system (Wells, 2005; Buckhoff, 2006; Coenen, 2008). Sales skimming can be conducted during non-business hours without the knowledge of the owners, where the fraudster can pocket the money for personal use (Wells, 2005; Buckhoff, 2006). Other ways for committing this scheme is stealing unrecorded cheques and substituting them for cash or understating sales by either reducing the item price or recording the sale of fewer items and stealing the excess receipts (Wells, 2005; Coenen, 2009). On the other hand, receivables skimming can be committed by lapping customer accounts (Wells, 2005; Buckhoff, 2006; Coenen, 2009) or by stealing, destroying, or altering the account statements by changing the customer's address in the billing system causing the statements to return back to the fraudster's desk (Wells, 2005; Hopwood et al., 2008; Coenen, 2009).

In contrast cash larceny, which is the second sub-category of asset misappropriation, involves the theft of funds that are already recorded in a company's accounting system. Thus, cash larceny is called an on-book scheme (Wells, 2005; Silverstone and Sheetz, 2007; Coenen, 2009; ACFE, 2010). In cash larceny because the funds have already been recorded somewhere in the company's accounting system, action must be taken to conceal the theft. This might include something like entering a false refund into the cash register, voiding a transaction, or booking an adjustment in the accounting records. Most larceny schemes involve the theft of cash at the following situations: At the point of sale, from incoming receivables or from the victim company's bank deposit (Wells, 2005; Coenen, 2009). According to the 2010 ACFE report, the median loss caused by cash larceny was $100,000 and the percentage of reported cash larceny cases were about 9.8% of the total reported fraud cases worldwide. The report also showed that cash larceny schemes are more prevalent in small sized firms and in the banking/financial services sector. Cash larceny at the point of sale can be committed and concealed by many ways, such as: stealing by using someone else's access code (Wells, 2005; Buckhoff, 2006), stealing currency in very small amounts over an extended period of time so that theft can be credited to errors rather than fraud (Wells, 2005 and Coenen, 2009), altering the cash counts to make the cash on hand and the tape balance or by simply destroying the register tape (Wells, 2005; Buckhoff, 2006; and Coenen, 2009). It can also be committed by making false voids or refunds which cause the register tape to reconcile to the amount of cash on hand after theft (Wells, 2005; Buckhoff, 2006; Hopwood et al., 2008; Coenen, 2009). However, larceny from receivables can be committed by reversing entries to balance the victim company's accounts or destroying records to conceal the identity of the thief. As for larceny from deposits, this can be committed by stealing cash from the deposit on the way to the bank and altering the deposit slip so that it reflects a lesser amount. This can be concealed by deposit lapping or carrying the missing money as deposits in transit which will appear on the next month's bank statement (Wells, 2005; Buckhoff, 2006; Coenen, 2009).

The third sub-category of asset misappropriation is called 'fraudulent disbursement'. In this scheme, the perpetrator causes his/her organisation to disburse funds through some tricks or devices (Wells, 2005; Buckhoff, 2006; Silverstone and Sheetz, 2007; ACFE,

2010). Figure 1 shows that fraudulent disbursement has further five sub-categories: billing schemes, cheque tampering schemes, payroll schemes, expense reimbursement schemes, and register disbursement schemes.

*Billing scheme* is any scheme in which a person causes his employer to issue a payment by submitting invoices for fictitious goods or services or goods with inferior quality, inflated invoices, or invoices for personal purchases (Wells, 2005; Buckhoff, 2006; Silverstone and Sheetz, 2007; ACFE, 2010). Results from the 2010 ACFE's *Report to the Nation on Occupational Fraud and Abuse*, showed the median loss caused by billing schemes is $128,000 and billing scheme cases accounted for 26% of the total reported fraud cases worldwide. The report also showed billing scheme cases occurred more in small sized firms rather than large sized ones and it tended to occur more in the manufacturing sector, followed by government and public administration sector. Billing scheme can be committed by creating shell companies, which is basically a fake company, that issue invoices to the victim company for products or services never delivered or provided (Silverstone and Sheetz, 2007; Vona, 2008; Coenen, 2009). The shell company can also inserts an intermediary into a company's transaction in order to overcharge the company and keep the profits. This can be concealed through fictitious authorisation (Wells, 2005; Coenen, 2009). Other ways for committing and concealing billing schemes include; altering the invoice of a legitimate vendor to cause the company to pay more than is really owed and getting the excess money by contacting the vendor and explaining a mistake has happened so that the fraudster could take the money for his personal use (Silverstone and Sheetz, 2007; Coenen, 2009), or this could happen in collusion with the vendor (Vona, 2008). Billing schemes can also be committed by making fictitious purchases by submitting a false invoice or approval, or by collusion with a real company, or by purchasing fictitious services rather than goods such as consulting services which is difficult to be traced (Wells, 2005; Buckhoff, 2006; Vona, 2008; Daigle et al., 2009).

The second sub-category of fraudulent disbursements is called *Cheque tampering* and it can be defined as any scheme in which a person steals his employer's funds by intercepting, forging, stealing, or altering a cheque drawn on one of the organisation's bank accounts (Wells, 2005; Vona, 2008; Coenen, 2009; ACFE, 2010). Although online banking, money transfers, and debit/credit cards are more commonly used nowadays in most countries including Egypt, cheques are still used by companies as a method of payment. The ACFE (2010) reported a median loss from cheque tampering of about $131000. The report also showed that cheque tampering is more prevalent in banking/financial services sector and that it is more likely to occur in small businesses. This can be committed if an authorised employee with the proper authority signs cheques for her/his personal use, by forging the signature of the person authorised to sign cheques, intercepting a cheque by signing the endorsement line, forging the company's name on the endorsement line, stealing and altering the payee name by using erasable ink in the initial preparation of the cheques with the intent to alter it after management's approval, or getting management to sign a blank cheques (Wells, 2005; Vona, 2008).

The third sub-category of fraudulent disbursements is *payroll scheme*. In this scheme, an employee causes his employer to issue a payment by making false claims for compensation (Wells, 2005; Silverstone and Sheetz, 2007; ACFE, 2010). As reported by the ACFE (2010), the median loss caused by payroll scheme was about $72,000. The report showed that cases from payroll scheme account for 8.5% of total reported fraud

cases worldwide. The report also showed that payroll scheme is more likely to occur in small businesses and in the manufacturing and public administration sectors alike.

Payroll fraud in case of hourly paid salaries can be committed if sales personnel misstate the sales amount to get more commission than what they deserve (Wells, 2005; Coenen, 2009), or by adding a fictitious person or failing to remove the name of a retired employee who used to work for the company which is called a ghost employee (Wells, 2005; Buckhoff, 2006; Silverstone and Sheetz, 2007; Coenen, 2008, 2009; Vona, 2008). It can also be committed by forging the necessary approval and then forwarding the forged timecard directly to payroll accounting by passing his/her supervisor (Wells, 2008; Coenen, 2009), or colluding to misstate the hours worked or altering time cards after being properly approved (Vona, 2008). Salaried employees can commit payroll fraud by generating fraudulent wages via increasing their rates of pay and forging their supervisor's approval, or by simply colluding with their supervisor, or recording fictitious year-end sales (Wells, 2005; Buckhoff, 2006; Vona, 2008; Coenen, 2009). In case of sales personnel whose salary depends on the amount of sales made, payroll fraud can be committed and concealed by changing quotes to get bonuses, falsifying the amount of sales by creating fictitious sales, recording a higher price in the company book than what was actually charged to a customer, increasing the rate of commission, or changing the prices listed on sales documents (Wells, 2005; Coenen, 2009). Other methods include; selling sales promotional items or causing sales to be recorded early (Vona, 2008).

However in *expense reimbursement schemes*, which are the fourth sub-category of fraudulent disbursements schemes, an employee makes a claim for reimbursement of fictitious or inflated business expenses (Wells, 2005; Buckhoff 2006; Coenen, 2009; ACFE, 2010). Median loss caused by expense reimbursement fraud scheme, as reported by the ACFE (2010), is $33,000. The report also showed that expense reimbursement scheme accounts for 15% of all reported fraud cases and it was more likely to occur in small businesses and more prevalent in the manufacturing sector. It can be committed by claiming items that do not qualify under the company's reimbursement policy, and concealing the true nature of the expenses to ensure they are approved, reporting multiple expenses just below the threshold requiring receipts, creating fake expense items to generate a cash reimbursement, altering receipts using a correction fluid, or obtaining blank receipts from vendors. Other ways include charging something on the company-paid credit card, and then submitting the receipt separately to obtain a cash reimbursement, duplicating receipt for a meal and submitting that one after the original receipt was already reimbursed, or expensing personal items as if they were business expenses such as expensing personal vacations as business trips (Wells, 2005; Coenen, 2009).

The last sub-category of asset misappropriation is cash *register disbursement scheme* which can be defined as any scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash. It can be committed through either false voids or refunds (Wells, 2005; Buckhoff, 2006; Coenen, 2009). Results from the ACFE 2010 'Report to the Nation on Occupational Fraud and Abuse' showed that cash register disbursement caused a median loss of about $23,000 and that it is more prevalent in the retail sector followed by banking services sector. Reported register disbursement fraud cases account for 3% of total reported fraud cases worldwide. Results also showed that this scheme is more likely to be committed in small and large sized firms equally and that it is not only the least costly form of fraud, but also tended to be detected the soonest.

Register disbursement can be committed and concealed by making fictitious refunds or overstating refunds, or making false voids in the cash register. This can be concealed by destroying records to prevent management from determining the identity of the thief and cover up money missing from the drawer (Wells, 2005; Coenen, 2009).

## 3 Literature review and research questions

Reviewing the literature showed very few research studies into asset misappropriation, however, none of them mentioned how external auditors might detect asset misappropriation. For instance, Chapple et al. (2007) examined the relation between the occurrence of asset misappropriation and the strength of firm's corporate governance in Australia and their findings revealed that the likelihood of asset misappropriation increase when the Chief Executive Officers (CEO) also holds the position of chairperson of the board of directors. They also found that the greater the number of independent directors on the audit committee, the lower the level of fraud. Their results indicate that employing good corporate governance reduces the risk of the asset misappropriation. Consistently, Mustafa and Youssef (2010) investigated the relationship between the financial expertise of the audit committee and the incidence of asset misappropriation in publicly held companies using a sample of 28 publicly held companies in the USA who were experiencing asset misappropriation from 1987 to 1998, as well as 28 control companies matched according to size, industry, and time period. Results revealed that the higher the percentage of financial expert members and the higher the percentage of independent members in the audit committee, the lower the likelihood of asset misappropriation. However, both studies did not examine how asset misappropriation can be detected or the role of external audit in detecting asset misappropriation as a corporate governance mechanism.

In another study, Coram et al. (2008) examined whether organisations with an internal audit function are more likely to detect and self-report asset misappropriation than those without. Their study depended on fraud data from the 2004 KPMG fraud survey which reported fraud from 491 organisations in the private and public sectors across Australia and New Zealand. Results revealed that companies who have an in-house internal audit department are more likely to detect asset misappropriation than those who outsource the internal audit function. However, again they did not mention how asset misappropriation might be detected. In addition, their research has the following limitations. First, having internal audit might not be the only reason for less asset misappropriation because having internal audit might be associated with good governance and internal controls which might increase the propensity to detect and self-report asset misappropriation. Second, they argue that better controls including internal audit will be associated with a greater propensity to detect and self-report fraud, however it is possible that better controls will be associated with a greater propensity to prevent fraud, causing less overall detected and self-reported fraud. Majid et al. (2010) conducted a study in Malaysia to explore the opinions of local authority employees on the issue of asset misappropriation. Their findings revealed that the most likely assets to be misused in a local authority are vehicles and internet connection. They also found factors that might lead to asset misappropriation include inadequate or lack of internal control, lack of employee's fraud education, lack of independent cheques, override of existing controls, and lack of management reviews, attitude, and lack of awareness of the

dishonest acts. Besides, the majority of respondents in their study believed the likelihood of asset misappropriation in the future is increasing. However, their research was based on the perception of employees in local authorities, did not show the types of asset misappropriation or how to detect any, and did not mention the role of external auditors in detecting this fraud scheme. Another limitation in their study is that it was conducted on just one local authority which makes it difficult for their results to be generalised.

Only one study by Gullkvist and Jokipii (2012) examined whether internal auditors, external auditors, and economic crime investigators perceive the importance of red flags as significantly different across asset misappropriation and fraudulent financial reporting, as well as across within-subject categories. 471web-based surveys were collected from 471 internal auditors, external auditors, and economic crime investigators.

Findings revealed that significant differences in perceptions exist among the participant groups. Internal auditors report a higher perceived importance of red flags related to detecting asset misappropriation than those related to fraudulent financial reporting, whereas the economic crime investigators perceived red flags for fraudulent financial reporting as more important than that of asset misappropriation. External auditors reported equal perceived importance of red flags across the two fraud types as well as across within-subject categories. They provided a list of red flags for asset misappropriation and fraudulent financial reporting. However, they did not suggest weights to red flags in their list and did not mention how external auditors might respond to these red flags. Another weakness is the low response rate which affects the generalisation of the study results.

Reviewing the literature also showed no prior studies into asset misappropriation in the Egyptian context. In addition, critics of fraud professional audit standards (Casabona, and Grego, 2003; Hoffman and Zimbelman, 2009; Wells, 2004) argued that audit professional standards did not mention how external auditors can decide on the quality or weights of red flags for fraud which leads to ineffective and inefficient fraud risk assessments. Others (Pedneault, 2004; Smith and Baharuddin, 2005; Zimbelman, 1997; Glover et al., 2003; Zikmund, 2008; Brazel et al., 2010; McDonald and Banks, 1997; Hogan et al., 2008; Srivastava et al., 2009; Shelton et al., 2001) mentioned that the standards omitted specific guidance for responding to fraud once the fraud risk factors are identified and did not require all procedures to be followed but merely suggested that auditors consider implementing them which might lead to inconsistencies in applying fraud-related audit procedures.

In the mean time, the Public Company Accounting Oversight Board (PCAOB, 2007) issued a report in 2007 to determine external auditors' overall approach to the detection of financial fraud and response to fraud risk factors. Results revealed that in some situations, auditors fail to respond appropriately to fraud risk factors. Consistently, Hassink et al. (2010) and Hamersley et al. (2011) examined audit seniors' responses to fraud risk factors as a way of providing evidence about the effectiveness and efficiency of external auditors' fraud risk assessments and responses. Findings revealed that external auditors do not respond in an effective and appropriate way to heightened fraud risk. Dezoort and Harrison (2007) conducted an experimental study with 230 auditors from two Big 4 audit firms to evaluate whether auditors perceive different responsibility for detecting the three types of occupational fraud (fraudulent financial reporting, misappropriation of assets, and corruption). Findings revealed that external auditors give more recognition to financial reporting fraud than the other two types of fraud.

Consistently, Kassem and Higson (2012) reviewed academic research studies to explore the reasons behind the audit expectation gap, and to assess the efforts of standards' setters and external auditors in narrowing the gap and detecting fraud. The results of the review showed that the gap is still there due to limitations in the professional audit standards and because external auditors may not be exerting enough efforts to detect material misstatements arising from fraud. They explained that external auditors still need guidance on how to rank risk factors while considering the likelihood of fraud to the business, impact of the fraud if it occurs, and pervasiveness of the fraud if found. They added that the standards also provide very little guidance for external auditors on how to respond to heightened fraud risk factors which may lead to an ineffective fraud risk response and did not require all procedures to be followed but merely suggested that auditors consider implementing them which leads to inconsistency in the audit procedures used by different audit firms in response to these fraud risk factors. They also found that some external auditors still do not increase the extent of audit procedures or even change the nature of audit procedures in response to fraud risk assessments, inconsistently respond to identified fraud risk factors, do not modify the nature of their audit plans to make planned procedures more effective at detecting fraud in response to fraud risk as required by the standards, do not use professional scepticism, do not hold or document brainstorming sessions, and give more attention to fraudulent financial reporting than the other two types of fraud (asset misappropriation and corruption). This indicates external auditors need more fraud training and awareness as well as guidance on how to assess and respond to heightened fraud risk factors.

Thus, the scarcity of prior studies into asset misappropriation, the limitations in fraud professional audit standards especially when it comes to guidance for external auditors on fraud risk assessment and response, along with the lack of fraud research in the Egyptian context motivated the current study to explore asset misappropriation and provide external auditors with a tool that might help them detect material misstatements arising from asset misappropriation. The tool suggested by the current study is a framework that includes a list of red flags of asset misappropriation ranked according to their relative importance along with suggested audit procedures that might help external auditors properly assess and respond to material misstatement arising from asset misappropriation. Thus, the proposed framework is divided into two parts, *the first part* lists the most important fraud risk factors associated with each category of asset misappropriation and *the second part* includes audit procedures that can be used by external auditors in response to each fraud risk factor.

To develop the first part of the framework (list of the most important risk factors) the current study sought to answer the following two questions:

Q1 Do external auditors perceive red flags as an effective tool in detecting material misstatements arising from asset misappropriation?

Q2 Do external auditors perceive red flags across and within asset misappropriation categories equally important?

To develop the second part of the proposed framework, the current study sought to determine how external auditors in Egypt might respond to the heightened fraud risk factors arising from asset misappropriation. Thus, the third research question is:

Q3 How might external auditors in Egypt respond to fraud risk factors arising from asset misappropriation?

## 4 Research methods

The current study generally aims at expanding external auditors' knowledge of the nature and categories of asset misappropriation as well as providing them with a framework that might help them properly assess and respond to risk factors arising from asset misappropriation. The proposed framework was developed in three stages as explained below.

### *4.1 1st stage – developing the initial list of red flags*

The first stage in developing the framework involved building an initial list of red flags arising from asset misappropriation. This list was initially built using examples of fraud risk factors provided by SAS No. 99, ISA No. 240 and Wells (2005) text book: *Principles of Fraud Examination*. This yields a list of 70 red flags for all types of asset misappropriation. The list was further refined by 15 external audit managers working in an international audit office in Egypt, reducing the total number of red flags to 52. The criteria used to refine the list of red flags include removing any duplication of red flags to avoid redundancy and merging some red flags for simplification. One example is false voids and false refunds which are related to register disbursements schemes. Another example is forged, missing, or altered refund documents in case of skimming schemes (see Table 1). The rationale behind that was to increase the response rate by reducing the list of red flags so respondents will not be bored to think and answer questions related to red flags. This list was then used as a base for the questionnaire which sought external auditors' perception on the importance of red flags arising from asset misappropriation.

### *4.2 2nd stage – importance of red flags across and within asset misappropriation categories – questionnaire*

In order to get the perception of external auditors on the relative importance of red flags across and within asset misappropriation categories, a questionnaire was used. This questionnaire was based on the list of red flags developed in the first stage, and aimed at answering the first and second research questions (whether red flags are effective in detecting asset misappropriation and whether red flags across and within asset misappropriation categories are equally important). The questionnaire was pilot-tested by 15 audit managers working in one of the leading international audit firms in Egypt, and then refined in accordance with the feedback received from the pilot study. The modifications required were mainly about rephrasing some of the questions to make it easily understandable by respondents and also included a change in the layout of the questionnaire to make it more attractive for respondents but no change was required in the number and style of questions.

**Table 1** List of red flags for asset misappropriation

| *Red flag for skimming schemes* |
|---|
| High levels of discounts, adjustments, returns, and write offs. |
| Similarities between the customers' addresses, ID numbers, or tax numbers and those of employees especially those working in the accounts receivable department. |
| Currency or cheques detail on summary sheets did not reconcile to the deposit ticket. |
| Flat or declining revenue, ratio of cash sales to credit sales or to total sales decreasing. |
| Forged, missing or altered refund documents. |
| Cash sales or receipts differing from deposits on bank statements. |
| Cash deposits totals differing from normal or expected patterns, or missing deposit slips, sales invoices or increased use of petty cash fund. |
| Unusual journal entries or reconciling items. |
| Customers with no telephone numbers or tax ID number may have been created for use in posting improper entries to hide a skimming scheme. |
| A significant rise in the number or size of overdue accounts could be a result of an employee who steals customer payments without ever posting them, thus causing the accounts to be past due. |
| Personal cheques included in cash funds (swapping cheques for cash). |
| *Red flags for cash larceny* |
| If sales records have been destroyed, this could be a sign of larceny schemes. |
| Discrepancies between sales records and cash on hand. Large differences will normally draw attention but also be alert to a high frequency of small dollar occurrences because fraudsters sometimes steal small amounts in the hopes that they will not be noticed or that they will be too small to review. |
| The totals in bank deposit slip, the organisation's copy of the deposit slip, the remittance list, and the general ledger posting of the day's receipts did not match. |
| Any instance in which a deposit in transit exceeds the two day clear. |
| All journal entries in cash accounts that appear to be unique adjustments. |
| *Red flags for billing schemes* |
| Unexplained increases in the quantity of goods purchased. |
| Purchases that cannot be traced to inventory. |
| Significant increases in average unit price of goods purchased could signal pass-through schemes. |
| If there is a match between employee addresses and vendor addresses. |
| The existence of unfamiliar vendors. |
| Vendors with company names consisting only of initials can be a sign of fraud because in most fraud cases fraudsters use their first name initials to form a shell company. |
| Internal control deficiency such as allowing a person who processes payments to approve new vendors. |
| Large billings broken into multiple smaller invoices, each of which is for an amount that will not attract attention. |
| The mailing address on an invoice if it is a mail drop or a residential address, it may indicate the existence of a shell company scheme. |

**Table 1** List of red flags for asset misappropriation (continued)

| *Red flags for billing schemes* |
|---|
| Repeatedly billing for the same or similar amounts and if the perpetrator has purchase authority, these amounts will tend to be just below the perpetrator's approval limit. |
| An invoice that lacks detailed descriptions of the items for which the victim organisation is being billed. |
| Billing schemes will cause an organisation's expenses to exceed budget projections. |
| Billing causes an increase in expenses from previous years. |
| Billing schemes will also tend to cause an increase in cost of goods sold relative to sales and will tend to negatively impact profits. |
| Rapidly increasing purchases from one vendor or vendor billing more than one month. |
| *Red flags for cheque tampering* |
| Any cancelled cheques with more than one endorsement should be investigated, as should any non-payroll cheques that an employee has endorsed. That is because; to convert intercepted cheques the perpetrator may have to use a dual endorsement. |
| Cheques issued to cash have a higher incidence of fraud. |
| Cheques that are fabricated or stolen will many times not be in the same general sequence as the company's normal cheque sequence. |
| Cheques that are stolen will normally not appear in the vendor cheque register and thus will be seen as a gap in the cheque sequence. |
| In case of rotating the authorisation duty, if a cancelled cheques shows a signature from the wrong signer for the date of the disbursement, this could indicate fraud. |
| *Red flags for payroll schemes* |
| Ghost employees who have no physical address or phone number or who have the same social security number and bank account number on their files can be a red flag for fraud existence. |
| Significant budget overruns could signal payroll fraud. |
| The net payroll expense was lower than the funds actually issued because it did not include amounts paid to ghost employees. |
| The pay cheque summaries prepared for management approval can have different type face from those the system printed. |
| *Red flags for expense reimbursement schemes* |
| Receipts from a restaurant that are submitted over an extended period of time, yet are consecutively numbered. This tends to indicate that the employee has obtained a stack of blank receipts and is using them to support fictitious expenses. |
| Receipts or other support that do not looks professional or lack information about the vendor such as phone numbers, physical addresses, or logos. |
| Employees claiming items that were paid for in cash. Claiming an expense was paid in cash allows the fraudster to explain why there is no audit trail for the expense. |
| Using credit cards for low dollar amount expenses while using cash in higher dollar expenses |
| High usage of credit cards by certain employees may be a sign of abuse. |
| Expenses that are consistently rounded off, ending with a 0 or a 5 which tends to indicate that the employee is fabricating the numbers. |
| Patterns in which expenses are consistently for the same amount. For instance; a salesperson's business dinners always cost $120. |
| Reimbursement requests from an employee that consistently fall at or just below the organisation's reimbursement limit. |

**Table 1** List of red flags for asset misappropriation (continued)

| *Red flags for register disbursement schemes* |
|---|
| Missing or forged void or refund document. |
| Customer sales posted to one card and refunds posted to another card. |
| Increased void or refund transactions by individual employees. |
| Cashier's ability to issue refund without supervision. |
| The existence of some company's branches with high adjustments. |

The questionnaire was then delivered by hand to one hundred external auditors working in different types of audit firms in Egypt (local, international, and Big 4 international). However, 93 questionnaires were received, which is still a very high response rate compared to other research studies. Purposive sampling was used to choose the study sample because it allows access to as wide a range of individuals relevant to the research questions as possible so that many different perspectives and ranges of activity are the focus of attention (Fisher, 2004; Bryman, 2012). Purposive sampling was also used for two reasons. The first reason is the difficulty that was faced in accessing the audit firms and offices in Egypt and in convincing external auditors to fill the questionnaire. Thus, to increase the response rate, personal contacts was used to reach the study respondents and to make sure they personally filled the questionnaire. The second reason pertains to highly technical questions that require respondents who have sufficient years of experience and qualifications. This was important to the current study because if respondents have insufficient knowledge or experience, they may deliberately guess at the answer, a tendency known as 'uninformed response' which reduces the reliability of data.

The questionnaire was about eight pages including a cover letter which was addressed to the applicant. The cover letter includes the research purposes and importance, and a request of cooperation from the part of the applicants in completing the practical part of the research (see Appendix A2). It also includes a statement that ensures the confidentiality in using the responses of the applicants and that it will only be used for academic research purpose. The questionnaire was divided into three main sections. The first section was designed to answer the first research question (Do external auditors perceive red flags of asset misappropriation effective in detecting material misstatements arising from asset misappropriation?). Questions in this section are closed-ended questions and the nominal scale are used providing only two alternative answers that each respondent is requested to choose from (yes or no). Closed questions facilitate the processing of data because they are normally pre-coded, thus reducing coding errors and time (Bryman, 2012). They also enhance the comparability of answers, and reduce the possibility of variability in the recording of answers. The second section was designed to answer the second research question (Do external auditors perceive red flags across and within categories of asset misappropriation equally important?). Respondents in this section were asked to rank the list of red flags for each category of asset misappropriation on a scale from 1 to 5, where '1' denotes the least important red flag and '5' denotes the most important red flag. The third section includes questions about respondents demographic factors (years of experience and type of audit office) as well as a question seeking the permission of respondents to interview them later. This was used as a basis for choosing more participants for the interview in addition to personal contacts.

Tables 2 and 3 show the distribution of the study sample in terms of their audit years of experience and type of audit office. As shown in Table 2, out of 93 respondents, only 88 respondents filled information about their years of audit experience, but all of them mentioned the type of their audit office as shown in Table 3.

**Table 2** Respondents' years of audit experience

| *Years of audit experience* | *(0–2) years* | *(3–5) years* | *(6–10) years* | *More than 10 years of experience* |
|---|---|---|---|---|
| Respondents | 26 | 31 | 13 | 18 |

**Table 3** Respondents' type of audit office

| *Types of audit office* | *Local* | *International* | *Big 4* |
|---|---|---|---|
| Respondents | 16 | 75 | 2 |

### *4.3 3rd stage – fraud risk response-interview*

The third stage in building the proposed framework was to get respondents' views on the likely audit procedures that be used in response to red flags of asset misappropriation. In order to reach this step and answer the third research question (How external auditors could respond to heightened fraud risk factors?), an interview was conducted with 20 external auditors (eight audit seniors and 12 audit managers) working in an international audit office in Egypt. To get the sample for the interview, snowballing was used. Thus, initially personal contacts was used to get access to that audit firm and to interview five external auditors in the population who have considerable years of audit experience to be able to answer highly technical questions about the audit procedures. These five respondents (all audit seniors) were further asked to identify other respondents who might be interested in being interviewed and who also have similar years of audit experience. This added up more ten respondents who were interested to be interviewed (three audit seniors and seven audit managers). Another five respondents from the questionnaire in the second stage showed interest to be interviewed and they were all audit managers.

The interview was semi-structured interview, including predetermined set of questions (How would you likely respond to each of the below red flags of asset misappropriation?) but the answers were not predetermined in order to allow respondents to answer freely without restricting their thoughts to a number of choices. This better served the purpose of the research because the research aimed to get every possible audit procedure that experienced external auditors may use to respond to heightened fraud risk factors arising from asset misappropriation.

Interviewees were given the refined list of red flags for asset misappropriation developed in stage two and they were asked to mention every possible audit procedure(s) they might use as a response to each red flag under each category of asset misappropriation. Interviewees were provided with a credible rationale for the research in which they are being asked to participate and for giving up their valuable time. An introductory statement was made to show the importance of the research and the kind of information to be collected and why they have been selected. Respondents were reassured that their identity will be anonymised and any information provided will be confidential. The interview was tape-recorded to ensure validity and reliability, and to

keep track of interviewees' responses. Each interview took about 50 minutes. The results of the interview were then refined by removing similar audit procedures and adding every possible audit procedure in front of each heightened fraud risk factor. This yielded a framework of categories of asset misappropriation, red flags of each, and related audit procedures (see Section 6). To ensure credibility participants was given relevant information before the interview via e-mail. This enabled interviewees to consider the information being requested and allowed them the opportunity to assemble supporting organisational documentation from their files.

## 5 Data analysis and research results

### *5.1 Questionnaire*

Data collected from the questionnaire was analysed using SPSS. Frequency tables were used including the number of observations recorded for each separate question in each section and sub section as well as the percentages of responses to determine external auditors' perception on the importance of red flags of asset misappropriation (see Appendix A1). The questionnaire was mainly used to test the first and second research questions. Below are the results of the analysis.

#### *5.1.1 1st research question*

The first research question was about whether external auditors perceive red flags as an effective tool in detecting asset misappropriation. To test respondents' answers to the first question, descriptive statistics (frequency tables and median) were used. Results showed that 58% to 97% of respondents perceived that the suggested list of red flags of skimming schemes is important for detecting such fraud scheme. The median score for these red flags was 57%, which means 57% or more of these red flags were perceived important in detecting skimming schemes.

As for red flags of cash larceny schemes, results showed that 72% to 98% of respondents perceived the suggested list of red flags of cash larceny important in detecting such fraud scheme. The median score showed that 62.4% or more of the suggested red flags for cash larceny were perceived important in detecting this type of fraud.

On the other hand, results for the subcategories of fraudulent disbursement schemes showed that 58% to 97% of respondents believe the suggested red flags for billing schemes are important, with a median score of 57%. Results also showed that 60% to 95% of respondents perceived red flags for cheque tampering important in its detection, with a median score of 69.9%. As for payroll schemes, 65% to 96% of respondents perceived red flags for this type as important in its detection (median = 66.7%). Red flags for expense reimbursement schemes got from 53% to 90% acceptance from respondents and a median score of 53.8%. Red flags of the last type of fraudulent disbursement schemes, register disbursements, got from 86% to 95% percentage of acceptance from respondents and a median score of 61.3%. The above results indicate that external auditors in Egypt perceive red flags as an effective tool in detecting material misstatements arising from asset misappropriation. This also shows that external auditors in Egypt are aware of the red flags associated with different categories of asset misappropriation.

### *5.1.2 2nd research question*

The second research question sought to determine whether external auditors perceive red flags across and within the different categories of asset misappropriation equally important. Data was analysed using SPSS and frequency tables were used. Analysis of the results revealed that external auditors did not perceive red flags of asset misappropriation equally important. This was inconsistent with results from Gullkvist and Jokipii (2012) who found equal perceptions of external auditors of the red flags for each subcategory in asset misappropriation. For instance, in skimming schemes, the most important red flags were: 'forged or missing refund or accounts receivable documents', 'increased customer complaints', and 'collection of written off accounts receivable without recording'.

The study results were consistent with results from the 'ACFE 2010 Report to the Nation on Occupational Fraud and Abuse', and 'KPMG 2006, 2007 Fraud Survey' where tips from customers were found the most commonly cited method for fraud detection. Thus, if external auditors paid more attention to tips from customers and encouraged management to implement a proper control system for handling such complaints, more skimming schemes might be detected. On the other hand, 'decreasing payments on accounts receivable' and 'a discrepancy in cash totals from normal patterns' were perceived as the least important red flags. This might be because decreasing payments on accounts receivable can be due to an ineffective credit policy inside the company or because clients are having financial problems that hinder them from paying their liabilities. Also, discrepancies in cash deposit totals may be due to the company's increased use of cash in dealing with its transactions rather than fraud.

In case of cash larceny, results revealed that the most acceptable red flags were: 'stealing the amount of collected cash sales and recording an amount which is less than what was actually collected', 'the totals in bank deposit slip, the organisation's copy of the deposit slip, the remittance list, and the general ledger posting of the day's receipts did not match', and 'discrepancies between cash sales records in the company and cash on hand available in the company's safes'. However, the least acceptable red flags were: 'deposits in transit that show up on bank reconciliation for more than two days', and 'the existence of customers' cash invoices among credit invoices for customers'.

As for billing schemes, which is the first type of fraudulent disbursements schemes, results showed that the most acceptable red flags for billing schemes were: 'internal control deficiency', 'purchases that cannot be traced to inventory', and 'recording some fixed assets such as equipments and supplies twice where the first as fixed assets and the second as expenses'. The least acceptable red flags were: 'the existence of a match between the employees address and the vendor's address', and 'rapidly increasing purchases from one vendor'. This was consistent with results from the ACFE 2010 Report, KPMG 2006, 2007 Fraud surveys, where deficiencies in internal control was cited as the most common reason for fraud. It was also consistent with Chapple et al. (2007) who found that the risk of asset misappropriation decrease with a strong system of internal control. On the other hand, the most acceptable red flags for cheque tampering were: 'the existence of a cheque that shows a signature from the wrong signer for the date of the disbursement', 'cheque issued to cash, and cheque that do not appear in the vendor cheque register', while the least acceptable red flags were: 'the existence of any cancelled cheques with more than one endorsement or any non-payroll cheque that an employee has endorsed', 'the company does not keep all cancelled cheques', and 'lack of

supporting documents for actually receiving the cheques'. This was quite surprising as some of these red flags like 'lack of supporting documents for actually receiving the cheques' should arouse the auditors' attention and should have been highlighted as one of the most important red flags for cheque tampering. However, this may be because cheques are not the most common method of payment in Egypt nowadays and external auditors might not be exposed enough to audit them.

Regarding payroll schemes, the most acceptable red flags were: 'recording fake amounts for employees' transportation expense, expenses for employees' stay, or wages for temporary employees and stealing those amounts', 'paying salaries to ghost employees who have any missing needed personal details', and 'the existence of temporary and changing employment inside the company'. However, the least acceptable red flags were: 'significant budget overruns', 'the pay cheque summaries prepared for management approval having different type face from those printed by the system', and 'payment of amounts to employees in excess of their stated salaries and wages included in the company's payroll sheet'.

As for the other two types of fraudulent disbursements schemes, the most acceptable red flags for expense reimbursement were: 'receipts from a restaurant that are submitted over an extended period of time yet are consecutively numbered', 'supporting documents that do not look professional or lack any needed information about the vendor', and 'using only copies of invoices and not original invoices when reimbursing expenses'. The least acceptable red flags were: 'high usage of credit cards by a certain employee compared to his colleagues', 'reimbursement requests from an employee that consistently fall at or just below the organisation's reimbursement limit', and 'expenses that are rounded off, ending with a 0 or 5 indicating that the value was fabricated'.

In case of register disbursements schemes, the most acceptable red flags were: 'missing or forged void or refund document', 'cashier's ability to issue refunds without supervision', and 'the existence of some of the company's branches with high adjustments'. However, the least acceptable red flags were: 'increased void or refund transactions by individual employees', and 'customer sales posted to one card and refunds posted to another card'.

To sum up, respondents did not perceive red flags across and within each category equally important and Table 4 shows these red flags ranked according to their relative importance in an ascending order, where the most important red flag was mentioned first and given the number '1', the second important red flag was given the number '2', and so on.

### *5.1.3 3rd research question*

In order to answer the third research question (How might external auditors in Egypt respond to risk factors arising from asset misappropriation?), an interview was conducted with 20 external auditors (eight audit seniors and 12 audit managers) working in an international audit office in Egypt. Each respondent was asked to state the possible audit procedure(s) he/she might in response to the list of red flags of asset misappropriation that was provided to them in the interview. Their responses were then analysed manually and refined by omitting repeated audit procedures so that for each red flag there will be one or more possible audit procedure.

**Table 4** Ranked red flags of asset misappropriation

| | *Red flag for skimming schemes* |
|---|---|
| 1 | Personal cheques included in cash funds (swapping cheques for cash) |
| 2 | Unusual journal entries or reconciling items |
| 3 | Cash deposits totals differing from normal or expected patterns, or missing deposit slips, sales invoices or increased use of petty cash fund. |
| 4 | Cash sales or receipts differing from deposits on bank statements. |
| 5 | Forged, missing or altered refund documents |
| 6 | Flat or declining revenue, Ratio of cash sales to credit sales or to total sales decreasing. |
| 7 | Currency or cheque detail on summary sheets did not reconcile to the deposit ticket. |
| 8 | Similarities between the customers' addresses, ID numbers, or tax numbers and those of employees especially those working in the accounts receivable department |
| 9 | High levels of discounts, adjustments, returns, and write offs. |
| 10 | A significant rise in the number or size of overdue accounts could be a result of an employee who steals customer payments without ever posting them, thus causing the accounts to be past due. |
| 11 | Customers with no telephone numbers or tax ID number may have been created for use in posting improper entries to hide a skimming scheme. |
| | *Red flags for cash larceny* |
| 1 | All journal entries in cash accounts that appear to be unique adjustments. |
| 2 | Any instance in which a deposit in transit exceeds the two day clear |
| 3 | The totals in bank deposit slip, the organisation's copy of the deposit slip, the remittance list, and the general ledger posting of the day's receipts did not match. |
| 4 | Discrepancies between sales records and cash on hand. Large differences will normally draw attention but also be alert to a high frequency of small dollar occurrences because fraudsters sometimes steal small amounts in the hopes that they will not be noticed or that they will be too small to review. |
| 5 | If sales records have been destroyed, this could be a sign of larceny schemes. |
| | *Red flags for billing schemes* |
| 1 | Rapidly increasing purchases from one vendor or vendor billing more than one month. |
| 2 | Large billings broken into multiple smaller invoices, each of which is for an amount that will not attract attention. |
| 3 | Internal control deficiency such as allowing a person who processes payments to approve new vendors. |
| 4 | Vendors with company names consisting only of initials can be a sign of fraud because in most fraud cases fraudsters use their first name initials to form a shell company. |
| 5 | The existence of unfamiliar vendors. |
| 6 | If there is a match between employee addresses and vendor addresses. |
| 7 | Significant increases in average unit price of goods purchased could signal pass-through schemes. |
| 8 | Purchases that cannot be traced to inventory. |
| 9 | Unexplained increases in the quantity of goods purchased. |
| 10 | Billing schemes will also tend to cause an increase in cost of goods sold relative to sales and will tend to negatively impact profits. |
| 11 | Billing causes an increase in expenses from previous years. |

**Table 4** Ranked red flags of asset misappropriation (continued)

| | |
|---|---|
| | *Red flags for billing schemes* |
| 12 | Billing schemes will cause an organisation's expenses to exceed budget projections. |
| 13 | Repeatedly billing for the same or similar amounts and if the perpetrator has purchase authority, these amounts will tend to be just below the perpetrator's approval limit. |
| 14 | The mailing address on an invoice if it is a mail drop or a residential address, it may indicate the existence of a shell company scheme. |
| 15 | An invoice that lacks detailed descriptions of the items for which the victim organisation is being billed. |
| | *Red flags for cheque tampering* |
| 1 | Cheques that are stolen will normally not appear in the vendor cheque register and thus will be seen as a gap in the cheques sequence. |
| 2 | Cheques that are fabricated or stolen will many times not be in the same general sequence as the company's normal cheques sequence. |
| 3 | Cheques issued to cash have a higher incidence of fraud. |
| 4 | Any cancelled cheques with more than one endorsement should be investigated, as should any non-payroll cheque that an employee has endorsed. That is because; to convert an intercepted cheque the perpetrator may have to use a dual endorsement. |
| 5 | In case of rotating the authorisation duty, if a cancelled cheques shows a signature from the wrong signer for the date of the disbursement, this could indicate fraud. |
| | *Red flags for payroll schemes* |
| 1 | The pay cheque summaries prepared for management approval can have different type face from those the system printed |
| 2 | The net payroll expense was lower than the funds actually issued because it did not include amounts paid to ghost employees. |
| 3 | Significant budget overruns could signal payroll fraud. |
| 4 | Ghost employees who have no physical address or phone number or who have the same social security number and bank account number on their files can be a red flag for fraud existence |
| | *Red flags for expense reimbursement schemes* |
| 1 | High usage of credit cards by certain employees may be a sign of abuse. |
| 2 | Using credit cards for low dollar amount expenses while using cash in higher dollar expenses |
| 3 | Employees claiming items that were paid for in cash. Claiming an expense was paid in cash allows the fraudster to explain why there is no audit trail for the expense. |
| 4 | Receipts or other support that do not looks professional or lack information about the vendor such as phone numbers, physical addresses, or logos. |
| 5 | Receipts from a restaurant that are submitted over an extended period of time, yet are consecutively numbered. This tends to indicate that the employee has obtained a stack of blank receipts and is using them to support fictitious expenses |
| 6 | Reimbursement requests from an employee that consistently fall at or just below the organisation's reimbursement limit. |
| 7 | Patterns in which expenses are consistently for the same amount. For instance, a salesperson's business dinners always cost $120. |
| 8 | Expenses that are consistently rounded off, ending with a 0 or a 5 which tends to indicate that the employee is fabricating the numbers. |

**Table 4** Ranked red flags of asset misappropriation (continued)

| | *Red flags for register disbursement schemes* |
|---|---|
| 1 | Missing or forged void or refund document |
| 2 | Cashier's ability to issue refund without supervision |
| 3 | The existence of some company's branches with high adjustments |
| 4 | Increased void or refund transactions by individual employees |
| 5 | Customer sales posted to one card and refunds posted to another card |

Results from the interview revealed that external auditors in Egypt suggested the use of analytical procedures, review of reconciling items, inquiries of management, employees, and vendors, examination of ledgers and journal entries, surprise audit visits, physical count, confirmation, documentation, and re-performance in response to red flags arising from asset misappropriation. It was also noticed that most interviewees suggested the extensive use of analytical procedures, including comparisons, simple analysis (summary reports), trend analysis, and horizontal analysis, in case of skimming schemes, billing schemes, payroll schemes, expense reimbursement schemes, and register disbursement schemes. For instance, in skimming schemes five interviewees suggested the auditor compare total receipts with results of daily physical count and daily deposits with banks in case cash deposits totals differ from normal or expected patterns or in case of missing deposit slips, sales invoices or increased use of petty cash. Three interviewees suggested the auditor match the customer master file to the employee master file to spot similarities between customers' details and employees' details especially those working in the accounts receivable department. Automated systems like IDEA are more likely to help external auditors make this match in no time. One interviewee suggested the auditor run reports summarising the number of discounts, adjustments, and write offs generated by location, department, or employee to highlight high levels of discounts, adjustments, returns, and write offs. Again, automated systems can help external auditors to run these reports. In addition, six interviewees believed trend analysis on aging of customer accounts is the best procedure to highlight significant rises in the number or size of overdue accounts. In case of billing schemes, analytical procedures were extensively suggested too. For instance, three interviewees believed auditors should compare quantities in billings with those recorded in the warehouse addition slips in case there are large billings broken into multiple smaller invoices. Another interviewee suggested comparing current price lists with those of vendors and with price lists in previous years to highlight significant increases in average unit price of goods purchased. Four other interviewees also suggested the use of analytical procedures to ensure adequacy in the amounts of cost of goods sold and to review purchase levels. Only one interviewee suggested management's inquiry in case an invoice lacks detailed descriptions of the items purchased.

However, the use of analytical procedures was not suggested in case of cash larceny schemes and cheque tampering. Alternatively, interviewees suggested documentation and management's inquiries in case of cash larceny. This might be because cash larceny is an on book scheme which means it is committed after recording transactions so it makes sense that examining documents could highlight any discrepancies or irregularities. For instance, one interviewee suggested auditor examines the general ledger details and all journal entries to cash accounts to highlight journal entries with unique adjustments.

Also, since the preparation of documents and financial statements is the responsibility of management, management's inquiry was one of the most suggested procedures in case of cash larceny. This inquiry could alert auditors to management's philosophy and operating style as well as the strength of management's control system when it comes to preparation and custody of important documents. For instance, five interviewees suggested the use of management's inquiry to know the reason behind a delay in deposits in transit, or in case of discrepancies between bank deposit slip and the general ledger of daily receipts, or in case of discrepancies between sales records and cash on hand. External auditors, as mentioned by Wells (2005), should also pay attention to small differences between sales records and cash on hand because fraudsters sometimes steal small amounts in the hopes that they will not be noticed or that they will be too small to review given external auditors normally pay attention to material amounts. Management's inquiry was also suggested in case sales records have been destroyed as this might be a sign of larceny. Two other interviewees suggested auditors should also advise management to reconstruct the records that have been destroyed to review the results of such transactions. Most interviewees agreed that management's inquiries has to be supported by documents as a kind of proof given management's inquiries is a weak audit procedure and should not be counted on alone.

As for cheque tampering, documentation and physical examination were the only suggested audit procedures by all interviewees. For instance, three interviewees suggested auditor examine the vendor cheques' register to search for gaps in the cheque sequence which might be a sign of stolen cheques or to spot cheques issued to cash which might be a sign for high incidence of cheque tampering fraud. Two interviewees suggested auditor investigate the reasons behind the dual endorsement. This can be through management's inquiry, or checking the company policy. Five interviewees saw reviewing supporting documents for cancelled cheques can be a way for checking proper authorisation on cancelled cheques.

In case of payroll schemes, six interviewees suggested the use physical examination of payroll data files and human resource documents to cheques the legality of employees' information. Two other interviewees suggested the use of re-performance and recalculation to ensure net pay agree with company records. While three interviewees suggested the use of analytical procedures, specifically trend analysis to spot significant budget overruns. As for expense reimbursement schemes, interviewees suggested a group of procedures including the use of credit summary reports that show and sort the usage of credit cards by employees, analysis of the type and nature of expenses to examine credit cards usages, checking the legality of receipts by visiting vendor's premises, or reviewing the company's reimbursement policy to ensure the legality of reimbursed expenses. One interviewee also mentioned that the use of companies' credit cards to cover travel expenses is not common in Egypt. The use of analytical procedures appeared to be useful also in case of false voids and refunds. Interviewees suggested examining sales system register and summarising refunds and voids by location can easily spot false voids and refunds. Another interviewee added that examining the sales system register can also help auditors check whether a customer sales posted to one card and refunds was posted to another as this is a signal for false voids and refunds. Other audit procedures suggested by the interviewees are summarised in Table 5 which explains the proposed framework for detecting asset misappropriation.

**Table 5** Framework for detecting asset misappropriation

| *Fraud category* | *Definition* | | *Red flags* | *Audit procedures* |
|---|---|---|---|---|
| Skimming | Theft of funds that took place before money is recorded in books | 1 | Personal cheques included in cash funds (attempt to swap cheques for cash) | Physical examination – surprise cash counts and getting proof of the cash available |
| | | 2 | Unusual journal entries or reconciling items | Review journal entries and reconciling items |
| | | 3 | Cash deposits totals differing from normal or expected patterns, or Missing deposit slips, sales invoices or increased use of petty cash fund. | Analytical procedures – compare total cash receipts with results of daily physical count and daily deposits with banks |
| | | 4 | Cash sales or receipts differing from deposits on bank statements. | Review bank reconciliations |
| | | 5 | Forged, missing or altered refund documents | Inquire management to find who forged or altered the refund documents |
| | | 6 | Flat or declining revenue, ratio of cash sales to credit sales or to total sales decreasing. | Inquire management and compare current year results with previous year, budget, and industry to understand the reasons behind these variances |
| | | 7 | Currency or cheque detail on summary sheets did not reconcile to the deposit ticket. | Reviewing bank reconciliations |
| | | 8 | Similarities between customers and employees details (sign of lapping scheme) | Analytical procedures – match the customer master file to the employee master file |
| | | 9 | High levels of discounts, adjustments, returns, and write offs. | Run reports summarising the number of discounts, adjustments, and write offs generated by location, department, or employee or review reconciling items and allowances and match sales returns with original sales or confirm sales returns with customers |
| | | 10 | A significant rise in the number or size of overdue accounts | Conduct trend analysis on aging of customer accounts or examine the 'customer statement report file' which is used to print customer statements and the opened sales invoices for that customer or Join the customer statement report file to accounts receivable and review for balance differences |
| | | 11 | Customers with no telephone numbers or tax ID number (sign for posting improper entries to hide a skimming scheme) | Examine customer master file and extract customers with no phone or tax ID number and ask management to send interim customer statements to ensure accuracy of customers account balances (confirmation) |

**Table 5** Framework for detecting asset misappropriation (continued)

| *Fraud category* | *Definition* | | *Red flags* | *Audit procedures* |
|---|---|---|---|---|
| Cash larceny | Theft of funds already recorded in books | 1 | All journal entries in cash accounts that appear to be unique adjustments. | Examine general ledger details and all journal entries to cash accounts |
| | | 2 | Deposit in transit exceeds the two day clear | Inquire management about the reason for this delay. |
| | | 3 | The totals in bank deposit slip, the organisation's copy of the deposit slip, the remittance list, and the general ledger posting of the day's receipts did not match | Inquire management about such discrepancies and review supporting documents for cash transactions. |
| | | 4 | Discrepancies between sales records and cash on hand | Inquire management and support response with documents otherwise issue a qualified or an adverse opinion depending on the materiality of the missing cash, and ask management to take remedial actions to stop occurrence of such differences |
| | | 5 | Sales records have been destroyed | Inquire management and make more investigations to ensure what happened was due to error and not fraud, and advise management to reconstruct the records showing the results of such transactions |
| | | 1 | Rapidly increasing purchases from one vendor or vendor billing more than one month | Confirm the legality of vendor by using the phone directory or by visiting the vendor's premises. |
| | | 2 | Large billings broken into multiple smaller invoices, each of which is for an amount that will not attract attention | Compare quantities in billings with those recorded in the warehouse addition slips |
| | | 3 | Internal control deficiency such as allowing a person who processes payments to approve new vendors | Increase control risk, advise management to make better controls, and report this deficiency in the management letter and to the audit committee or board of directors |
| | | 4 | Vendors with company names consisting only of initials (sign for shell company) | Advise management to confirm that those vendors actually exist by visiting the vendors' premises or by searching for their phone numbers in the phone directory |
| | | 5 | The existence of unfamiliar vendors | Check their addresses or visit their premises to confirm their existence |
| | | 6 | A match between employee addresses and vendor addresses | Inquire employee and the vendor about their address to ensure that no fraud exists |
| | | 7 | Significant increases in average unit price of goods purchased | Compare with other vendors' prices and with past purchase price of similar goods by the company |
| | | 8 | Purchases that cannot be traced to inventory | Physical count as the non-existent goods will cause inventory shortages |

**Table 5** Framework for detecting asset misappropriation (continued)

| *Fraud category* | *Definition* | *Red flags* | | *Audit procedures* |
|---|---|---|---|---|
| Billing schemes | Causing employer to issue a payment by submitting fake invoices, fake goods or services, inflated invoices, or invoices for personal use | 9 | Unexplained increases in the quantity of goods purchased | Ask for a technical report confirming the reasons beyond such increase |
| | | 10 | An increase in cost of goods sold relative to sales | Review purchase levels and use analytical procedures to ensure adequacy of such balances compared with previous year and the industry |
| | | 11 | An increase in expenses from previous years | Conduct horizontal analysis which is a comparison of financials on a year-to-year basis in case of a small company and analyse expense trends on a departmental or project basis in case of a large company |
| | | 12 | Organisation's expenses exceed budget projections | Compare between actual expenses and budgeted ones and if there is large difference, investigate the reasons by management inquiry |
| | | 13 | Repeatedly billing for the same or similar amounts or billing amounts just below the perpetrator's approval limit | Sort payments by vendor and amount. A software like IDEA can help in that |
| | | 14 | The mailing address on an invoice is a mail drop or a residential address (sign for shell company) | Check the sales history of this vendor to the company to know whether he is an old or a new vendor to the company, then visit vendor's company to ensure existence. If vendor is a fake one, inform an appropriate level of management about the matter to take the required actions |
| | | 15 | An invoice that lacks detailed descriptions of the items for which the victim organisation is being billed | Inquire management and ask for a duplicate invoice with all the needed details |
| Cheque tampering | Stealing employer's funds by intercepting, forging, stealing, or altering a cheque drawn on company's bank account | 1 | A gap in the cheque sequence (sign for missing cheques) | Examine the cheque register to search for these gabs |
| | | 2 | Cheques issued to cash | Examine the cheques register and extract all cheques payable to cash and summarise by issuer for reasonableness |
| | | 3 | Cancelled cheques with more than one endorsement or any non-payroll cheque that an employee has endorsed | Investigate the reasons behind the dual endorsement and examine company policy for endorsement |
| | | 4 | Cancelled cheques shows a signature from the wrong signer for the date of the disbursement | Review supporting documents for such check and compare the signature found with the signature of the authorised signer during such period |

**Table 5** Framework for detecting asset misappropriation (continued)

| *Fraud category* | *Definition* | *Red flags* | | *Audit procedures* |
|---|---|---|---|---|
| Payroll schemes | Causing employer to issue a payment by making false claims for compensation | 1 | The paycheque summaries prepared for management approval have different type face from those the system printed | Examine payroll data files and human resource documents to cheques legality of employees' information |
| | | 2 | The net payroll expense was lower than the funds actually issued (Sign for ghost employees) | Re-perform and recalculate the net pay for agreement to company records, recalculate the hours reported per the time card system to highlight any differences that may signal fraud, and examine employee master file and payroll records to compare current year to prior year payroll file or extract employee payments with payment dates after termination dates to detect additional or terminated employees or compare net payroll – to payroll cheques issued or compare current year to prior year payroll file to detect changes in pay rates or make exception reports testing for any employee whose compensation have increased from the prior year by a disproportionately large percentage |
| | | 3 | Significant budget overruns | Conduct trend analysis by comparing Payroll expenses to budgeted amounts or prior years' totals or examine the payroll register to calculate the percentage of overtime to gross pay on a person-by-person basis and sort from low to high to highlight potentially high unauthorised employee payments |
| | | 4 | Employees who have no physical address or phone number or who have the same social security number and bank account number on their files (ghost employees) | Compare the personnel and payroll records |
| Expense reimbursement | Employee making a claim for reimbursement of fictitious or inflated business expenses | 1 | High usage of credit cards by certain employees | Summarise credit card use by employee and sort from high to low and analyse the type and nature of expenses |
| | | 2 | Using credit cards for low dollar amount expenses while using cash in higher dollar expenses | Analyse the type and nature of expenses |
| | | 3 | Employees claiming items that were paid for in cash to justify why there is no audit trail for the expense | Investigate the nature of such expense and its relation to the company's activity |
| | | 4 | Receipts or other support that do not looks professional or lack information about the vendor such as phone numbers, physical addresses, or logos | Check the legality of the vendor by visiting his premises or by checking his phone number in the phone directory |

**Table 5** Framework for detecting asset misappropriation (continued)

| *Fraud category* | *Definition* | | *Red flags* | *Audit procedures* |
|---|---|---|---|---|
| | | 5 | Receipts from a restaurant that are submitted over an extended period of time, yet are consecutively numbered | Check the nature of such expenses and its relationship with the company's activities and confirm legality of invoices with restaurants |
| | | 6 | Reimbursement requests from an employee that consistently fall at or just below the organisation's reimbursement limit | Review the company's reimbursement policy to ensure the legality of these reimbursed expenses and assess the nature of the company's reimbursed expenses to ensure its relationship with the company's operations |
| | | 7 | Patterns in which expenses are consistently for the same amount | Investigate the reason behind this ask for any supporting documents for these expenses and ask about the extent by which these expenses are related to the company's activities |
| | | 8 | Expenses that are consistently rounded off, ending with a 0 or a 5 which tends to indicate that the employee is fabricating the numbers | Examine invoice payment |
| Register disbursement | Making false entries on cash registers to conceal fraudulent removal of cash | 1 | Missing or forged void or refund document | Management's inquiry |
| | | 2 | Cashier's ability to issue refund without supervision | Management's inquiry |
| | | 3 | The existence of some company's branches with high adjustments | Examine sales system register and summarise by location all refunds and voids charged |
| | | 4 | Increased void or refund transactions by individual employees | Summarise by location all refunds and voids charged |
| | | 5 | Customer sales posted to one card and refunds posted to another card | Examine the sales system registers |

## 6 Proposed framework for detecting asset misappropriation

The current study sought to provide auditors with knowledge about asset misappropriation which has rarely been investigated in prior literature. It also sought to provide external auditors with a framework that might help them detect material misstatements arising from asset misappropriation. This framework was developed in three stages. The first stage was an initial list of 70 red flags associated with each category of asset misappropriation. This was derived from Wells (2005) text book about fraud examination which covers a wide variety of fraud cases occurring in the USA and in many other countries, as well as, examples of red flags of asset misappropriation provided by ISA No. 240 and SAS No. 99. This list was then refined by 15 external audit managers working in an international audit office in Egypt. This yields a list of 52 red flags of asset misappropriation which was later used as a base for the questionnaire in the second stage of the framework development.

The second stage necessitates ranking the refined list of red flags from stage one according to their relative importance based on the perceptions of 93 external auditors in Egypt having proper audit experience. This stage answers the first two research questions (whether red flags are effective in detecting asset misappropriation and whether they have the same importance across and within asset misappropriation categories). Thus, this part fill an important gap in prior literature and address a limitation in fraud audit professional standards which is showing the rank or the relative importance of red flags associated with a type of fraud that has rarely been investigated in prior literature. The third step focus on audit procedures or the likely responses of external auditors to the heightened red flags of asset misappropriation. This also addresses another gap in the literature as well as a limitation in the current fraud audit professional standards (providing little guidance to external auditors on how to respond to heightened fraud risk factors). To develop this part of the framework, the current study interviewed eight audit seniors and 12 audit managers in one of the international audit offices in Egypt. The interviewees were asked about their likely responses to the red flags under each category of asset misappropriation. Their responses were then analysed and merged to the list of ranked red flags to develop the framework as shown in Table 5.

Thus, the framework includes a definition of each category of asset misappropriation, red flags, and the likely response to heightened red flags as shown in Table 5. Although this framework was based on perceptions of external auditors in Egypt, it can still be used by external auditors in any other country because the list of red flags was derived from examples provided by fraud audit professional standards that are applied by different countries. In addition the list was based on Wells' textbook which includes real fraud cases that took place in different countries. However, this framework could later be applied and empirically tested to determine its applicability in different audit environments.

## 7 Conclusions

Fraud is a major concern for investors, regulators, and external auditors. Standards setters issued fraud audit standards to meet the public's concerns and to expand external auditor's responsibility for detecting two types of fraud, asset misappropriation and fraudulent financial reporting. However, standards setters' efforts did not succeed in

meeting the public's expectations because it provided little guidance to external auditors as to how to respond to fraud risk factors and did not assign weights for red flags. This might lead to an inefficient and ineffective fraud risk assessment and fraud risk response. Reviewing the literature also showed very few research studies into asset misappropriation. However, none of them mentioned how asset misappropriation could be detected by external auditors. Hence, to address this gap, the current study focuses on asset misappropriation, provides insights into a type of fraud that has had little examination in prior literature, and develops a framework that might help external auditors properly assess and respond to risk factors arising from asset misappropriation. This framework consists of a ranked list of red flags for each category of asset misappropriation along with the likely audit procedures or response to each of these red flags. Thus, the current study contributes to both literature and practice by providing knowledge about a type of fraud that has seldom been investigated in prior literature and by developing a framework that might help external auditors in detecting material misstatements arising from asset misappropriation while addressing two limitations in professional fraud audit standards (giving weights to red flags and providing guidance to external auditors on how to respond to these red flags). This will in turn reduce the audit expectation gap and raise the profile of the audit profession as well as reduce the probability of audit firms' legal liability for negligence in detecting material misstatements due to fraud.

The proposed framework in the current study also shows that analytical procedures were perceived to be useful in detecting all categories of asset misappropriation except for cash larceny and cheque tampering which respondents suggested might be detected using management's inquires supported by documentation. Other procedures that was suggested by interviewees as a response for red flags of asset misappropriation include physical examination, review of reconciliations, confirmation, examination and review of supporting documents, journal entries, and ledgers, re-performance and recalculation, and conducting surprise audit visits to vendors' and clients' premises. Results from the questionnaire also revealed that external auditors in Egypt view red flags as an effective tool in detecting material misstatements arising from asset misappropriation. However, they did not perceive all red flags of the different categories of asset misappropriation equally important. For example, results from the current study showed that one of the most important red flags for skimming scheme as perceived by respondents is increased customer complaints which is consistent with results from the 'ACFE 2010 Report to the Nation on Occupational Fraud and Abuse', and 'KPMG 2006, 2007 Fraud Survey' where tips from customers were found the most commonly cited method for fraud detection. Thus, if external auditors paid more attention to tips from customers and encouraged management to implement a proper control system for handling such complaints, more fraud would be detected. Results also showed that among the most acceptable red flags for billing schemes was 'internal control deficiency which is also consistent with results from the ACFE 2010 Report, KPMG 2006, 2007 Fraud surveys, where deficiencies in internal control was cited as the most common reason for fraud. This was also consistent with Chapple et al. (2007) who found less incidence of asset misappropriation when there is a strong internal control or corporate governance. However, the current study's results was inconsistent with results from Gullkvist and Jokipii (2012) where external auditors had equal perceptions of the importance of red flags for each sub-category of asset misappropriation.

Like any other study, the current research has limitations. One of its limitations is that only two respondents in the study worked for the Big 4 international audit firms while most of our sample was from local and international firms. Hence, the results cannot be generalised to all external auditors in Egypt. However, this was due to the difficulty in accessing Big 4 audit firms in Egypt. Another limitation is the use of basic statistical analysis rather than models and sophisticated statistical techniques. The proposed framework was also based on perceptions of external auditors in Egypt and was not empirically tested. However, this was the first attempt in the literature to design a tool that might help external auditors in detecting material misstatements arising from asset misappropriation. Thus, future research should try to empirically test the framework developed in this study to determine how effective it is in helping external auditors detect material misstatements due to asset misappropriation in different audit environments.

## References

Alleyne, P. and Howard, M. (2005) 'An exploratory study of auditors' responsibility for fraud detection in Barbados', *Managerial Auditing Journal*, Vol. 20, No. 1, pp.1–26 [online] http://www.emeraldinsigh.com (accessed 1 June 2012).

Association of Certified Fraud Examiners (ACFE) (2002) *Report to the Nation on Occupational Fraud and Abuse*, pp.1–42 [online] http://www.acfe.com (accessed 1 June 2012).

Association of Certified Fraud Examiners (ACFE) (2010) *Report to the Nation on Occupational Fraud and Abuse*, pp.1–40 [online] http://www.acfe.com (accessed 1 June 2012).

Association of Certified Fraud Examiners (ACFE) (2012) *Report to the Nation on Occupational Fraud and Abuse*, pp.1–43 [online] http://www.acfe.com (accessed 1 June 2012).

Bayley, S.A. and Eliff, D.N. (2009) 'Fraud detection', *Oil and Gas Investor*, Vol. 29, No. 5 [online] http://www.proquest.com (accessed 12 July 2012).

Brazel, J.F., Jones, K.L. and Prawitt, D.F. (2010) *Improving Fraud Detection: Do Auditors React to Abnormal Inconsistencies between Financial and Nonfinancial Measures?*, Working Paper [online] http://www.ssrn.com (accessed 2 July 2012).

Bryman, A. (2012) *Social Research Methods*, 4th ed., Oxford University Press, New York.

Buckhoff, T. (2006) 'Fraud detection', *American Accounting Association Conference Proceedings*, August, Washington, DC, USA.

Casabona, P. and Grego, M. (2003) 'SAS 99 – consideration of fraud in a financial statement audit: a revision of statement on auditing standards 82', *Review of Business*, Vol. 1, Spring [online] http://www.ebscohost.com (accessed 15 July 2012).

Chapple, L., Fergusion, C. and Kang, D. (2007) *Corporate Governance and Misappropriation*, Working Paper [online] http://www.ssrn.com (accessed 15 July 2012).

Coenen, T.L. (2008) *Essentials of Corporate Fraud*, John Wiley & Sons, Inc., New Jersey.

Coenen, T.L. (2009) *Expert Fraud Investigation: A Step-by-Step Guide*, John Wiley and Sons, Hoboken, New Jersey.

Coram, P., Ferguson, C. and Moroney, R. (2008) 'Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud', *Accounting and Finance*, Vol. 48, No. 2, pp.543–559.

Dahawy, K., Shehata, N.F. and Ransopher, T. (2010) 'The state of accounting in Egypt: a case', *Journal of Business Cases and Applications*, Vol. 1, No. 3, pp.1–12.

Daigle, R., Morris, P.W. and Hayes, D.C. (2009) 'Small businesses: know the enemy and their methods', *The CPA Journal*, Vol. 79, No. 10, pp.30–38 [online] http://www.proquest.com (accessed 5 April 2012).

Dezoort, T. and Harrison, P. (2007) *The Effects of Fraud Type and Accountability Pressure on Auditor Fraud Detection Responsibility and Brainstorming Performance*, Working paper, December, pp.1–24 [online] http://www.ssrn.com (accessed 5 April 2012).

Elder, R.J., Beasley, M.S. and Arens, A.A. (2010) *Fraud Auditing. Auditing and Assurance Services: An Integrated Approach*, 13th ed., Pearson, New Jersey.

Fisher, C. (2004) *Researching and Writing a Dissertation for Business Students*, Prentice Hall, Edinburgh Gate, UK.

Glover, S.M., Prawitt, D.F., Schultz, J.J. and Zimbelman, M.F. (2003) 'A test of changes in auditors' fraud-related planning judgments since the issuance of SAS No. 82', *Auditing: A Journal of Practice & Theory*, Vol. 22, No. 2, pp.237–251.

Gullkvist, B. and Jokipii, A. (2012) 'Perceived importance of red flags across fraud types', *Critical Perspectives on Accounting*, Vol. 1, No. 3, pp.1–18 [online] http://www.elsevier.com (accessed 28 July 2012).

Hamersley, J.S., Johnstone, K.M. and Kadous, K. (2011) 'How do audit seniors respond to heightened fraud risk?', *Auditing: A Journal of Practice & Theory*, Vol. 30, No. 3, pp.81–101 [online] http://www.aaa.com (accessed 15 July 2012).

Hassan, O. and Power, D.M. (2009) 'The usefulness of accounting information: evidence from the Egyptian market', *Qualitative Research in Financial Markets*, Vol. 1, No. 3, pp.125–141 [online] http://www.emeraldinsights.com (accessed 3 July 2012).

Hassink, H., Meuwissen, R. and Bollen, L. (2010) 'Fraud detection, redress and reporting by auditors', *Managerial Auditing Journal*, Vol. 25, No. 9, pp.861–881.

Hoffman, V.B. and Zimbelman, M.F. (2009) 'Do strategic reasoning and brainstorming help auditors change their standard audit procedures in response to fraud risk?', *The Accounting Review*, Vol. 84, No. 3 [online] http://www.aaa.com (accessed 15 July 2012).

Hogan, C.E., Rezaee, Z., Riley, R. and Velury, U.K. (2008) 'Financial statement fraud: insights from the academic literature', *Auditing: A Journal of Practice & Theory*, Vol. 27, No. 2, pp.231–252.

Hopwood, W.S., Leiner, J.J. and Young, G. (2008) *Forensic Accounting*, McGraw-Hill Irwin, New York.

International Auditing Standards Board (2009) *The Auditors' Responsibilities Relating to Fraud in an Audit of Financial Statements*, International Standards on Auditing No. 240 [online] http://www.iaasb.org (accessed 15 July 2012).

Johnson, G.G. and Rudesill, C.L. (2001) 'An investigation into fraud prevention and detection of small businesses in the United States: responsibilities of auditors, managers, and business owners', *Accounting Forum*, Vol. 25, No. 1.

Jones, M. (2011) *Creative Accounting, Fraud, and International Accounting Scandals*, John Wiley and Sons Ltd., The Atrium, Southern Gate, Chichester.

Kassem, R. and Higson, A.W. (2012) 'Financial reporting fraud: are external auditors and standards' setters doing enough?', *International Journal of Business and Social Sciences*, October, Vol. 3, No. 19, pp.283–290.

KPMG (2007) 'Profile of a fraudster survey' [online] http://www.kpmg.org (accessed 15 July 2012).

KPMG Forensics (2006) 'Fraud survey' [online] http://www.kpmg.org (accessed 15 July 2012).

Lasko, A.D. (2009) 'Preventing damaging effects of asset misappropriation', *Debt Cubed; Commercial Law League of America*, July/August [online] http://www.businesssourcepremier.com (accessed 15 July 2012).

Majid, R.A., Mohamed, N., Abdullah, A. and Mahmud, Z. (2010) 'An exploratory study on the possibility of misappropriation of assets occurring in a local authority', *International Conference on Science and Social Research*, Kuala Lumpur, Malaysia, 5–7 December, pp.36–41.

McDonald, D.K. and Banks, G.Y. (1997) 'Implementing the new fraud auditing standard in your auditing practice', *Ohio CPA Journal*, Vol. 56, No. 3, pp.26–31.

Mustafa, S.T. and Youssef, N.B. (2010) 'Audit committee financial expertise and misappropriation of assets', *Managerial Auditing Journal*, Vol. 25, No. 3, pp.208–225.

O'Gara, J.D. (2004) *Corporate Fraud: Case studies in Detection and Prevention*, John Wiley and Sons, Incorporated, Hoboken, NJ, USA [online] http://www.ebrary.com/lib/bue (accessed 15 July 2012).

Pedneault, S.A. (2004) 'Yes, auditors can stop fraud, if they know what to look for', *White-Collar Crime Fighter*, Vol. 6, No. 8, pp.1–3.

PricewaterhouseCoopers (PWC) (2010) 'The global economic crime survey: economic crime in a downturn' [online] http://www.pwc.org (accessed 15 July 2012).

PricewaterhouseCoopers (PWC) (2011) 'Cybercrime: protecting against the growing threat – global economic crime survey', November [online] http://www.pwc.com (accessed 15 July 2012).

Public Company Accounting Oversight Board (PCAOB) (2007) Observations on Auditors' Implementation of PCAOB Standards Relating to Auditors' Responsibilities with Respect to Fraud [online] http://www.pcaob.com (accessed 15 July 2012).

Shelton, S.W., Whittington, O.R. and Landsittel, D. (2001) 'Auditing firms' fraud risk assessment practices', *Accounting Horizons*, Vol. 15, No. 1, pp.19–33.

Silverstone, H. and Sheetz, M. (2007) *Forensic Accounting and Fraud Investigation for Non-Experts*, 2nd ed., John Wiley & Sons, Inc., Hoboken, New Jersey.

Smith, M. and Baharuddin, I. (2005) 'Auditors' perception of fraud risk indicators: Malaysian evidence', *Managerial Auditing Journal*, Vol. 20, No. 1, pp.73–85.

Soltani, B. (2007) 'Corporate fraud, corporate scandals, and external auditing', *Auditing: An International Approach*, Pearson Education Limited, Edinburgh.

Srivastava, R.P., Mock, T.J. and Turner, J.L. (2009) 'Bayesian fraud risk formula for financial statement audits', *Abacus: A Journal of Accounting, Finance, and Business Studies*, Vol. 45, No. 1, pp.66–80.

Vona, L.W. (2008) *Fraud Risk Assessment: Building a Fraud Audit Program*, John Wiley and Sons, Hoboken, New Jersey.

Wells, J.T. (1995) 'Report to the nation on occupational fraud and abuse' [online] http://www.acfe.com (accessed 15 July 2012).

Wells, J.T. (2004) *Occupational Fraud and Abuse*, Obsidian Publishing, Austin, Texas.

Wells, J.T. (2005) *Principles of Fraud Examination*, John Wiley and Sons, Hoboken, New York.

Zikmund, P.E. (2008) 'Reducing the expectation gap', *CPA Journal*, Vol. 78, No. 6, pp.20–25.

Zimbelman, M.F. (1997) 'The effects of SAS No. 82 on auditors' attention to fraud risk factors and audit planning decisions', *Journal of Accounting Research*, Vol. 35, No. 2, pp.75–97.

Zweighaft, D. (2004) 'Slicing the salami: small-dollar recurring fraud', *Journal of Investment Compliance*, Fall, Vol. 1, pp.138–140.

## Appendix

### *A1 Analysis of the results*

| *Median for red flags associated with skimming schemes* | | |
|---|---|---|
| | *Frequency* | *Percent* |
| No | 40 | 43% |
| Yes | 53 | 57% |
| Total | 93 | 93% |
| *Median for red flags for cash larceny schemes* | | |
| | *Frequency* | *Percentage* |
| No | 35 | 37.60% |
| Yes | 58 | 62.40% |
| Total | 93 | 100% |
| *Median for red flags associated with billing schemes* | | |
| | *Frequency* | *Percent* |
| No | 40 | 43% |
| Yes | 53 | 57% |
| Total | 93 | 100 |
| *Median for red flags associated with cheque tampering* | | |
| | *Frequency* | *Percent* |
| No | 28 | 30.1 |
| Yes | 65 | 69.90% |
| Total | 93 | 100 |
| *Median for red flags associated with payroll schemes.* | | |
| | *Frequency* | *Percent* |
| Yes | 62 | 66.7% |
| No | 31 | 33.3 |
| Total | 93 | 100 |
| *Median for red flags associated with expense reimbursement* | | |
| | *Frequency* | *Percentage* |
| Yes | 50 | 53.8 |
| No | 43 | 46.2 |
| Total | 93 | 100 |
| *Median for red flags associated with register disbursement scheme* | | |
| | *Frequency* | *Percentage* |
| Yes | 57 | 61.30% |
| No | 36 | 38.7 |
| Total | 93 | 100 |

| *Respondents' years of experience and red flags for skimming schemes* | | | | | |
|---|---|---|---|---|---|
| | *(0–2)* | *(3–5)* | *(6–10)* | *More than 10 years* | *Total* |
| No | 13 (14.7%) | 14 (15.9%) | 6 | 6 | 40 |
| | | | –6.8 | –15.40% | –44.30% |
| Yes | 13 | 17 | 7 | 12 | 53 |
| | –33.30% | –34.70% | –14.30% | –24.50% | –55.70% |
| Total | 26 | 31 | 13 | 18 | 93 |
| | –29.50% | –35.20% | -14.80% | –20.50% | –100% |

| *Chi square test for red flags for skimming* | | |
|---|---|---|
| *Type of fraud* | *Value of chi square* | *Significance* |
| Skimming | 1.247 | 0.742 |

| *Respondents' years of experience and red flags for cash larceny* | | | | |
|---|---|---|---|---|
| | *2 years or less* | *5 years or less* | *10 years or less* | *More than 10 years* |
| No | 11 | 12 | 5 | 7 |
| | 31.40% | 34.30% | 14.30% | 20% |
| Yes | 15 | 19 | 8 | 11 |
| | 28.30% | 35.80% | 15.10% | 20.80% |
| Total | 26 | 31 | 13 | 18 |
| | 29.50% | 35.20% | 14.80% | 20.50% |

| *Chi square test for red flags for cash larceny* | | | |
|---|---|---|---|
| *Type of fraud* | *Pearson chi square* | *Contingency coefficient* | *Significance value* |
| Cash larceny | 100 | 34 | 0.992 |

| *Respondents' years of experience and red flags for fraudulent disbursements schemes* | | | | |
|---|---|---|---|---|
| *Fraudulent disbursement schemes* | *2 years of experience or less* | *5 years of experience or less* | *10 years of experience* | *More than 10 years of experience* |
| No | 14 | 17 | 5 | 8 |
| | 31.80% | 38.60% | 11.40% | 18.20% |
| Yes | 12 | 14 | 8 | 10 |
| | 27.30% | 31.80% | 18.20% | 22.70% |
| Total | 26 | 31 | 13 | 18 |
| | 29.50% | 35.20% | 14.80% | 20.50% |

| *Chi square test for red flags for fraudulent disbursements schemes* | | |
|---|---|---|
| *Type of fraud* | *Pearson chi square* | *Significance value* |
| Fraudulent disbursement | 1.359 | 0.715 |

| *Type of audit office and red flags for skimming* | | | |
|---|---|---|---|
| *Skimming schemes* | *The big 4 international audit firms* | *Local audit offices* | *Total* |
| No | 1 | 3 | 40 |
| | 1.10% | 3.20% | |
| Yes | 1 | 13 | 53 |
| | 1.10% | 14% | |
| Total | 2 | 16 | 93 |
| | 2.20% | 17.20% | |

| *Type of audit office and red flags for skimming* | | |
|---|---|---|
| *Type of fraud* | *Pearson chi square* | *Significance value* |
| Skimming | 4.644 | 0.098 |

| Type of office and red flags for cash larceny | | | | |
|---|---|---|---|---|
| *Cash larceny* | *The big 4 international audit firms* | *International audit firms other than the big 4* | *Local audit offices* | *Total* |
| No | 1 | 32 | 2 | 35 |
| | 1.10% | 34.40% | 2.20% | |
| Yes | 1 | 43 | 14 | 58 |
| | 1.10% | 74.10% | 15.10% | |
| Total | 2 (2.2%) | 75 (80.6%) | 16 (17.2%) | 93 |

| *Chi square for red flags for cash larceny* | | | |
|---|---|---|---|
| *Type of fraud* | *Pearson chi square* | *Contingency coefficient* | *Significance value* |
| Cash larceny | 5.246 | 0.231 | 0.073 |

| *Type of audit office and red flags for fraudulent disbursements* | | | | |
|---|---|---|---|---|
| *Red flags for fraudulent disbursement schemes* | *The big 4 international audit firms* | *International audit firms other than the big 4 audit firms* | *Local audit firms* | *Total* |
| No | 1 | 41 | 3 | 45 |
| | 1.10% | 44.10% | 3.20% | |
| Yes | 1 | 34 | 13 | 48 |
| | 1.10% | 36.60% | 14% | |
| Total | 2 | 75 | 16 | 93 |
| | 2.20% | 80.60% | 17.20% | |

| *Chi square test for red flags for fraudulent disbursement* | | | |
|---|---|---|---|
| *Type of fraud* | *Pearson chi square* | *Contingency coefficient* | *The significance value* |
| Fraudulent disbursement schemes | 6.817 | 0.261 | 0.033 |

## *A2 Questionnaire*

Dear respondents,

The current research is seeking to help external auditors in Egypt detect material misstatements arising from asset misappropriation which was seldom covered in prior literature. This issue has also never been investigated in the Egyptian context before, thus your kind participation will be greatly appreciated. Kindly be informed that data collected by the current study will only be used for research purposes and will not be revealed to any other party whatsoever without your prior approval. I am also assuring the anonymity of your responses and the confidentiality of your personal details.

The questionnaire includes three sections where each section aims to answer a specific research question. The first section is seeking your perception on whether red flags are effective in detecting asset misappropriation. In this section a list of red flags is provided and you are kindly required to state whether you agree or disagree that each red flag will be effective in detecting a category of asset misappropriation. Please let me know if something is not clear or requires further clarification. In the second section, you are kindly required to rank each of the red flags according to their relative importance in detecting asset misappropriation based on your audit experience and knowledge of fraud. The third section, however, includes some demographic information about your kind selves for data analysis purposes.

Thanks for your cooperation in advance.

Yours sincerely,

Rasha Kassem

E-mail: rasha.kassem40@gmail.com

*Section 1*

This section is seeking your perception on whether red flags are effective in detecting asset misappropriation. A list of red flags is provided below and you are kindly required to state whether you agree or disagree that each red flag will be effective in detecting a category of asset misappropriation. Please denote your choice by putting (x).

*Q1 Do you agree that each of the following red flags is effective in detecting asset misappropriation*

| *Red flag for skimming schemes* | *Yes* | *No* |
|---|---|---|
| High levels of discounts, adjustments, returns, and write offs. | | |
| Similarities between the customers' addresses, ID numbers, or tax numbers and those of employees especially those working in the accounts receivable department | | |
| Currency or cheque detail on summary sheets did not reconcile to the deposit ticket. | | |
| Flat or declining revenue, Ratio of cash sales to credit sales or to total sales decreasing. | | |
| Forged, missing or altered refund documents | | |
| Cash sales or receipts differing from deposits on bank statements. | | |
| Cash deposits totals differing from normal or expected patterns, or Missing deposit slips, sales invoices or increased use of petty cash fund. | | |
| Unusual journal entries or reconciling items | | |
| Customers with no telephone numbers or tax ID number may have been created for use in posting improper entries to hide a skimming scheme. | | |
| A significant rise in the number or size of overdue accounts could be a result of an employee who steals customer payments without ever posting them, thus causing the accounts to be past due. | | |
| Personal cheques included in cash funds (swapping cheques for cash) | | |
| *Red flags for cash larceny* | | |
| If sales records have been destroyed, this could be a sign of larceny schemes. | | |
| Discrepancies between sales records and cash on hand. Large differences will normally draw attention but also be alert to a high frequency of small dollar occurrences because fraudsters sometimes steal small amounts in the hopes that they will not be noticed or that they will be too small to review. | | |
| The totals in bank deposit slip, the organisation's copy of the deposit slip, the remittance list, and the general ledger posting of the day's receipts did not match. | | |
| Any instance in which a deposit in transit exceeds the two day clear | | |
| All journal entries in cash accounts that appear to be unique adjustments. | | |
| *Red flags for billing schemes* | | |
| Unexplained increases in the quantity of goods purchased. | | |
| Purchases that cannot be traced to inventory. | | |
| Significant increases in average unit price of goods purchased could signal pass-through schemes. | | |
| If there is a match between employee addresses and vendor addresses. | | |
| The existence of unfamiliar vendors. | | |

| |
|---|
| Vendors with company names consisting only of initials can be a sign of fraud because in most fraud cases fraudsters use their first name initials to form a shell company. |
| Internal control deficiency such as allowing a person who processes payments to approve new vendors. |
| Large billings broken into multiple smaller invoices, each of which is for an amount that will not attract attention. |
| The mailing address on an invoice if it is a mail drop or a residential address, it may indicate the existence of a shell company scheme. |
| Repeatedly billing for the same or similar amounts and if the perpetrator has purchase authority, these amounts will tend to be just below the perpetrator's approval limit. |
| An invoice that lacks detailed descriptions of the items for which the victim organisation is being billed. |
| Billing schemes will cause an organisation's expenses to exceed budget projections. |
| Billing causes an increase in expenses from previous years. |
| Billing schemes will also tend to cause an increase in cost of goods sold relative to sales and will tend to negatively impact profits. |
| Rapidly increasing purchases from one vendor or vendor billing more than one month. |
| *Red flags for cheque tampering* |
| Any cancelled cheques with more than one endorsement should be investigated, as should any non-payroll cheques that an employee has endorsed. That is because to convert an intercepted cheque the perpetrator may have to use a dual endorsement. |
| Cheques issued to cash have a higher incidence of fraud. |
| Cheques that are fabricated or stolen will many times not be in the same general sequence as the company's normal cheque sequence. |
| Cheques that are stolen will normally not appear in the vendor cheques' register and thus will be seen as a gap in the cheque sequence. |
| In case of rotating the authorisation duty, if cancelled cheques shows a signature from the wrong signer for the date of the disbursement, this could indicate fraud. |
| *Red flags for payroll schemes* |
| Ghost employees who have no physical address or phone number or who have the same social security number and bank account number on their files can be a red flag for fraud existence |
| Significant budget overruns could signal payroll fraud. |
| The net payroll expense was lower than the funds actually issued because it did not include amounts paid to ghost employees. |
| The pay cheque summaries prepared for management approval can have different type face from those the system printed |
| Red flags for expense reimbursement schemes |
| Receipts from a restaurant that are submitted over an extended period of time, yet are consecutively numbered. This tends to indicate that the employee has obtained a stack of blank receipts and is using them to support fictitious expenses |
| Receipts or other support that do not looks professional or lack information about the vendor such as phone numbers, physical addresses, or logos. |

| |
|---|
| Employees claiming items that were paid for in cash. Claiming an expense was paid in cash allows the fraudster to explain why there is no audit trail for the expense. |
| Using credit cards for low dollar amount expenses while using cash in higher dollar expenses |
| High usage of credit cards by certain employees may be a sign of abuse. |
| Expenses that are consistently rounded off, ending with a 0 or a 5 which tends to indicate that the employee is fabricating the numbers. |
| Patterns in which expenses are consistently for the same amount. For instance; a salesperson's business dinners always cost $120. |
| Reimbursement requests from an employee that consistently fall at or just below the organisation's reimbursement limit. |
| *Red flags for register disbursement schemes* |
| Missing or forged void or refund document |
| Cashier's ability to issue refund without supervision |
| The existence of some company's branches with high adjustments |
| Increased void or refund transactions by individual employees |
| Customer sales posted to one card and refunds posted to another card |

*Section 2*

In this section, you are kindly required to rank each of the red flags according to their relative importance in detecting asset misappropriation based on your audit experience and knowledge of fraud using 5 Likert scale, where '1' denotes most important, and '5' denotes least important.

*Q Do red flags have equal importance within asset misappropriation categories?*

| *Red flag for skimming schemes* | *1* | *2* | *3* | *4* | *5* |
|---|---|---|---|---|---|
| High levels of discounts, adjustments, returns, and write offs. | | | | | |
| Similarities between the customers' addresses, ID numbers, or tax numbers and those of employees especially those working in the accounts receivable department | | | | | |
| Currency or cheques detail on summary sheets did not reconcile to the deposit ticket. | | | | | |
| Flat or declining revenue, ratio of cash sales to credit sales or to total sales decreasing. | | | | | |
| Forged, missing or altered refund documents | | | | | |
| Cash sales or receipts differing from deposits on bank statements. | | | | | |
| Cash deposits totals differing from normal or expected patterns, or Missing deposit slips, sales invoices or increased use of petty cash fund. | | | | | |
| Unusual journal entries or reconciling items | | | | | |
| Customers with no telephone numbers or tax ID number may have been created for use in posting improper entries to hide a skimming scheme. | | | | | |

| |
|---|
| A significant rise in the number or size of overdue accounts could be a result of an employee who steals customer payments without ever posting them, thus causing the accounts to be past due. |
| Personal cheques included in cash funds (swapping cheques for cash) |
| *Red flags for cash larceny* |
| If sales records have been destroyed, this could be a sign of larceny schemes. |
| Discrepancies between sales records and cash on hand. Large differences will normally draw attention but also be alert to a high frequency of small dollar occurrences because fraudsters sometimes steal small amounts in the hopes that they will not be noticed or that they will be too small to review. |
| The totals in bank deposit slip, the organisation's copy of the deposit slip, the remittance list, and the general ledger posting of the day's receipts did not match. |
| Any instance in which a deposit in transit exceeds the two day clear |
| All journal entries in cash accounts that appear to be unique adjustments. |
| *Red flags for billing schemes* |
| Unexplained increases in the quantity of goods purchased. |
| Purchases that cannot be traced to inventory. |
| Significant increases in average unit price of goods purchased could signal pass-through schemes. |
| If there is a match between employee addresses and vendor addresses. |
| The existence of unfamiliar vendors. |
| Vendors with company names consisting only of initials can be a sign of fraud because in most fraud cases fraudsters use their first name initials to form a shell company. |
| Internal control deficiency such as allowing a person who processes payments to approve new vendors. |
| Large billings broken into multiple smaller invoices, each of which is for an amount that will not attract attention. |
| The mailing address on an invoice if it is a mail drop or a residential address, it may indicate the existence of a shell company scheme. |
| Repeatedly billing for the same or similar amounts and if the perpetrator has purchase authority, these amounts will tend to be just below the perpetrator's approval limit. |
| An invoice that lacks detailed descriptions of the items for which the victim organisation is being billed. |
| Billing schemes will cause an organisation's expenses to exceed budget projections. |
| Billing causes an increase in expenses from previous years. |
| Billing schemes will also tend to cause an increase in cost of goods sold relative to sales and will tend to negatively impact profits. |
| Rapidly increasing purchases from one vendor or vendor billing more than one month. |

| *Red flags for cheque tampering* |
|---|
| Any cancelled cheques with more than one endorsement should be investigated, as should any non-payroll cheques that an employee has endorsed. That is because to convert an intercepted cheques the perpetrator may have to use a dual endorsement. |
| Cheques issued to cash have a higher incidence of fraud. |
| Cheques that are fabricated or stolen will many times not be in the same general sequence as the company's normal cheque sequence. |
| Cheques that are stolen will normally not appear in the vendor cheques' register and thus will be seen as a gap in the cheque sequence. |
| In case of rotating the authorisation duty, if cancelled cheques shows a signature from the wrong signer for the date of the disbursement, this could indicate fraud. |
| *Red flags for payroll schemes* |
| Ghost employees who have no physical address or phone number or who have the same social security number and bank account number on their files can be a red flag for fraud existence |
| Significant budget overruns could signal payroll fraud. |
| The net payroll expense was lower than the funds actually issued because it did not include amounts paid to ghost employees. |
| The pay cheque summaries prepared for management approval can have different type face from those the system printed |
| Red flags for expense reimbursement schemes |
| Receipts from a restaurant that are submitted over an extended period of time, yet are consecutively numbered. This tends to indicate that the employee has obtained a stack of blank receipts and is using them to support fictitious expenses |
| Receipts or other support that do not looks professional or lack information about the vendor such as phone numbers, physical addresses, or logos. |
| Employees claiming items that were paid for in cash. Claiming an expense was paid in cash allows the fraudster to explain why there is no audit trail for the expense. |
| Using credit cards for low dollar amount expenses while using cash in higher dollar expenses |
| High usage of credit cards by certain employees may be a sign of abuse. |
| Expenses that are consistently rounded off, ending with a 0 or a 5 which tends to indicate that the employee is fabricating the numbers. |
| Patterns in which expenses are consistently for the same amount. For instance; a salesperson's business dinners always cost $120. |
| Reimbursement requests from an employee that consistently fall at or just below the organisation's reimbursement limit. |
| *Red flags for register disbursement schemes* |
| Missing or forged void or refund document |
| Cashier's ability to issue refund without supervision |
| The existence of some company's branches with high adjustments |
| Increased void or refund transactions by individual employees |
| Customer sales posted to one card and refunds posted to another card |

*Section 3*

This section includes some demographic information about your kind self which is needed for data analysis purposes only. I assure you that your information will remain confidential and will only be used for the purpose of this study.

How many years of audit experience you have? Please tick (x) in the right box

- 0–2 years ☐
- 3–5 years ☐
- 6–10 years ☐
- More than 10 years ☐

What is the type of your audit office? Please tick (x) in the right box

- Local audit office ☐
- International audit office ☐
- Big 4 audit office ☐

Please note if you would accept to be interviewed later to cooperate more in this research. Please tick (x) in the right box

- Yes I would like to be interviewed ☐
- No I do not like to be interviewed ☐

If you ticked 'Yes', please write your e-mail or mobile number:

Thanks for your cooperation