Macrothink Institute™

Case Studies in Business and Management
ISSN 2333-3324
2016, Vol. 3, No. 1

White Collar Fraud: A Case Study of KOSS

Gagan Kukreja (Corresponding Author)

Department of Accounting & Economics, College of Business & Finance

Ahlia University. P.O. Box 10878, Kingdom of Bahrain

E-mail: gkukreja@ahlia.edu.bh

Robert Brown

Management Consultant, Kingdom of Bahrain

E-mail: Robert9819@me.com

Received: February 28, 2016 Accepted: March 28, 2016 Published: April 7, 2016

doi:10.5296/csbm.v3i1.9116 URL: http://dx.doi.org/10.5296/csbm.v3i1.9116

Abstract

Fraud does not draw community and political reaction like other crimes (Chapman & Smith, 2001) yet many believe that fraud can be as serious or even more serious than certain types of street crimes (Rebovich & Kane, 2002). The financial statement fraud of KOSS, an American company of more than $34 million was discovered in 2009 after the tipoff from American Express to Michael Koss, CEO. The fraud was significant relative to the size, turnover and profit of the organization perpetrated by senior accounting professional (white collar). KOSS would be classified as an SME and this fraud emphasizes that it is not only large organizations that need to be vigilant regarding accounting frauds and internal controls, but smaller companies as well. Because of its size, KOSS had little segregation of duties and, as was later revealed, massive weaknesses in internal controls. The external auditors, (Grant Thornton, LLP or "GT") upon whom management were relying, did not have a full understanding of the business and clearly did not meet the expectations of senior management. It is also appeared that auditors failed to apply required audit standards during the audit. Later on, the external auditors agreed to pay KOSS compensation worth $8.5 million in July 2013 as a settlement.

The board of directors including audit committee appeared to be unconcerned regarding effective internal controls, risk management and (wrongly) assumed that they could trust their senior executive staff. The board's limited policy of ethics and compliance was outdated and did not include a whistleblowing policy. There was no internal audit function reporting to the

board. Further, the computerized accounting system was outdated and lacked the application controls found in more modern applications. The purpose of this case study is to analyze what went wrong at KOSS, who was involved in fraud and how such kind of frauds can be avoided in future.

Keywords: Accounting fraud, Internal control, Audit committee, Risk management, White collar fraud, Whistleblowing policy

1. Introduction to KOSS

KOSS is a well-known manufacturer of high-end headphones and is based in Massachusetts, USA. KOSS was established in 1971 and is primarily owned by Michael Koss and his family (who hold a share of around 79%). Koss designs and manufactures a vast variety of electronic items such as stereo headphones, computer headsets, speaker-phones, telecommunications headsets, active noise cancelling stereo headphones and wireless stereo headphones (Koss website). Products are sold through various channels under the KOSS name.

The company is considered to be small and according to the Securities & Exchange Commission ("SEC") filings, Koss had a market capitalization of less than $75 million and a total of 73 employees at the time when the fraud took place. Although the majority of KOSS stock is held by directors and executive officers, KOSS had become a public company through an indirect route, when founder, John Koss purchased a small public company in New York that was bankrupt. KOSS kept the NASDAQ listing and changed the trading name to KOSS. Therefore, KOSS was subject to the corporate governance requirements and SEC compliance that are applicable to listed companies in the USA (Koss website).

The purpose of this case study is to examine: What is fraud? How the fraud was detected and who were involved? What was modus operandi? Why the fraud was not detected for so long? How the internal control and oversight failures those lead to the fraud not being detected? The researchers will evaluate the role of other parties such as directors, executive management, auditors and regulators in preventing and detecting the fraud. The research will cover the broader implications of this fraud and the lessons that can be learned by the SME sector.

2. What is Fraud

Fraud is one of the biggest evils for any society. Fraud can inflict significant damage at community, organizational or individual level (Lanham et al., 1987), and the potential consequences of fraud for organizations can be strategic, legal, financial or operational. Therefore, it must be an important issue for any organization. In legal terms, fraud is a generic category of criminal conduct that involves the use of dishonest or deceitful means in order to obtain an unfair advantage or gain over another, in order to secure something of value or deprive another of a right (Smith, 2001). Many of times it is viewed as a victimless crime, fraud does not draw community and political reaction like other crimes (Chapman & Smith, 2001). Yet, while less dramatic than crimes of violence like murder or rape, many now people believe that fraud can be as serious as or even more serious than certain types of street crimes (Rebovich & Kane, 2002).

Frauds are highly destructive to free-market capitalism and, more broadly, to the underpinnings of society (Greenspan, 2002). In this information technology era, money in electronic form are much easier to steal: while US$1B in $100 bills occupies about 15 cubic meters, and in gold would weighs about 65 tons, in electronic form is just 32 bits plus some application-dependent headers (Parker, 1998). The fundamental principle of criminology is that crime follows opportunity (Grabosky et al., 2001), and opportunities for fraud abound in

today's world which is also happened in KOSS case as well. The ability to edit, alter or otherwise manipulate computerized data to derive benefit from its misrepresentation in a way that is often undetectable increases significantly the fraud opportunities (Smedinghoff, 1996).

Fraud is always intentional, intentional by appearance, or intentional by inference from the act. According to Brenner (2001), someone commits fraud if the following four elements are proved beyond a reasonable doubt:

a) *Actusreus*: The perpetrator communicates false statements to the victim;

b) *Mens rea*: The perpetrator communicates what she knows are false statements

c) with the purpose of defrauding the victim;

d) Attendant circumstances: The perpetrator's statements are false; and

e) Harm: The victim is defrauded out of property or something of value.

3. How the Fraud Occurred and Who Defrauded KOSS?

In the last quarter of 2009, it came to the light that Sujata Sachdeva, then the company's VP of Finance, Company Secretary and Principal Accounting officer, had misappropriated almost $34 million of funds over a period of five years. To put this in perspective, this amount equaled almost one year's turnover for KOSS and nearly half of its pretax profits for the period over which the fraud occurred. It is surprising that such a fraud could remain undetected for so long, particularly given its size in relation to its size and turnover. Ms. Sachdeva had misappropriated the following amounts over the period of 5 years: 2005 - $2,195,477; 2006 - $2,227,669; 2007 - $3,160,310; 2008 - $5,040,968; 2009 - $8,485,937; 2010 - $10,243,310 (first two quarters) (Koss Press Release, Dated January 11, 2010). As illustrated above, Ms. Sachdeva grew progressively bolder in terms of the amounts she misappropriated, realizing that her methods of concealing the fraud were working. She was very likely well aware of what the auditors would be looking for (and also what they were not looking for) and was able to hide the fraud based upon her position, knowledge, expertise and experience.

The SEC's complaint of August 30, 2010 provides details of the means used by Sachdeva to obtain cash by circumventing the internal controls. The indictment confirmed that Sachdeva used her position at KOSS to fraudulently obtain significant money from the company for personal gain. Julie Mulvaney, then the company's senior accountant assisted Sachdeva in covering up the fraud. The following factors are considered to have enabled the fraud to occur:

- As per the KOSS payment policies, Michael Koss was supposed to approve the invoices greater than $5,000, but no approval was needed for wire transfers or cashier's checks (the primary method of theft used by Sachdeva). It was serious lapse in payment policy.

- The accounting software was more than 30 years old, and did not lock the accounting records at the end of a month, to prevent later changes to the books of account. This

deliberate ignorance of adoption of latest software gives opportunities to Sachdeva to manipulate accounting records and hide the money theft from the company.

- Many account reconciliations were either not prepared, or were not maintained as part of KOSS's accounting records. To the extent that reconciliations were conducted, they were improperly performed by the either Sachdeva or Mulvaney who initiated or recorded the transactions, enabling those persons to make modifications to the reconciliations to cover up fraudulent entries. This was clear violation of segregation of duties and internal control override.

- While Sachdeva gave Michael J. Koss the financial statements for his review, he did not conduct an adequate review in connection with the required legal certifications, which caused lack of oversight. It creates serious problem of governance.

Sachdeva acknowledged misappropriating $15 million by formally sanctioning of issuance of more than 500 cashier's checks to pay her personal expenses. Cashier's checks were issued directly to retailers, such as Nieman Marcus and Saks Fifth Avenue, and other vendors. Sometimes acronyms were used, like N-M and S.F.A., in an attempt to disguise the identity of the payee. Further, Sachdeva fraudulently authorized and initiated numerous wire transfers of KOSS funds to KOSS's banker, American Express ("Amex") to pay for personal credit card. During 2008 and 2009, she fraudulently authorized more than 200 bank wire transfers totaling more than $16 million to Amex. Other methods of misappropriating included misuse of petty cash. She issued many "petty cash cheques" which were cashed by employees and money was returned to her. She also collected money from unused traveler's cheque that were returned by employees who travelled on company-related business, and fraudulently kept money for her own benefit.

She managed to disguise the theft in the cost of goods sold with the help of Mulvaney. This was because it was easy to justify an increase in cost of goods sold caused by rising material costs, and the auditors probably wouldn't have known enough about the industry and raw materials costs to question the increasing costs. By doing the same theft repeatedly, the cost of goods sold went up yearly by an amount that did not raise suspicions in the minds of the auditors, but the other executives, including Micheal should have been careful enough to look into the rise in the cost of goods sold as they had industry experience. As mentioned earlier, Ms. Sachdeva was assisted by her colleague in concealing the fraud.

It looks Mulvaney didn't get any money from the embezzlement, and she has not been charged with theft. But it seems clearly that she actively and materially participated in the disguising of the fraud and was therefore charged with civil fraud. As per the SEC complaint, both ladies were able to hide the material cash by recording top-side general journal entries.

The following specific methods were used to conceal the fraud:

- Mulvaney prepared a "red book" containing numerous false journal entries. She recorded the false journal entries in the red book and then entered them in the company's accounting books and records with adjusted amounts without supporting documentary evidences.

- Mulvaney also prepared falsified accounting books and maintained them in various color folders, called the "rainbow files". The rainbow files consisted of 7 folders covering years 1995-2000 (green), 2004 (orange), 2005 (blue), 2005 (orange), 2006 (blue), 2007 (yellow), and 2008 (green). These files included more than 100 fraudulent transactions.
- These files also displayed a scheme to conceal the receipt of funds through a debit/credit wipe ("DC wipe"). A DC wipe made it appear that certain transactions (e.g., a sale to a customer and the receipt of funds) never took place. For example, in December 2007, KOSS received funds totaling more than $100,000 from an overseas customer. Mulvaney falsified the books and records though DC. In order to avoid detection, Mulvaney reduced 5 another sales accounts by different amounts that collectively totaled the exact amount – instead of reducing a single sales account by the whole amount, which makes auditor work difficult to detect such fraud.
- Sachdeva & Mulvaney didn't record any sales in KOSS's books made over the Internet or at the company's retail outlet, totaling $1.8 million over 4 years by December 2010 (accountingweb.com). It is surprising if Mulvaney did not realize that something was amiss and equally surprising that she went along with the cover-up. There could be several reasons why she did this including:

  1) She might have initially not realized that the transactions she was booking were covering up a fraud and by the time she realized, a substantial amount of false accounting had occurred (although this does not seem plausible).

  2) Because of the above, she felt that if the fraud was discovered, she would partially share the blame. Also, the company did not appear to have any "whistle blowing" or "protected disclosure" policy or "independent internal audit". If the company had such a policy in place, she might have been more inclined to come forward.

  3) Sachdeva might have held a substantial position of power and made her feel that her job was at risk if she did not go along with the cover-up. The one thing that is clear is that the company did not have an established "whistle-blowing" policy or culture. Had this been in place, it might have provided Mulvaney the opportunity to raise concerns at an early stage without the fear of blame or retribution.

4. Why the Fraud Was Not Detected Earlier?

It is surprising that a fraud of this size (i.e., relative to the size of KOSS) was not detected earlier either by the senior management or by the auditors but was eventually detected after Amex who raised concerns about payments they received from KOSS for Ms. Sachdeva's personal charge card. Some possibilities include:

- The fact that Ms. Sachdeva was a "trusted" employee of the company and had been with the company for more than 15 years. Further, Ms. Sachdeva was colluding with Ms. Mulvaney to cover up the fraud.

- The fraud was committed in a variety of manners, including wire transfers to pay Amex, cashiers cheques that were endorsed to various vendors who had sold goods or provided services to Ms. Sachdeva and misappropriation of petty cash and travelers cheques.

- It appears that there were some key controls that were missing in the internal control process and that collusion occurred which overrode the control principal of segregation of duties and lack of control over authorization and approval of funds transfers and cheques. In an organization of this size, it would be expected that any monetary transaction of a significant amount should be authorized by a senior member of management (most likely Mr. Michael Koss himself).

- The fact that Mr. Michael Koss was under the impression that the company had a robust system of internal controls in place and did not realize that an internal audit function and close board oversight was needed.

- The fact that Mr. Michael Koss (and possibly other members of management) had a level of disdain for internal auditing, audit committees and internal controls and considered that their time would be better spent on more strategic activities.

- The external auditors (GT) being overly familiar with the organization and, perhaps not exercised the due level of professional skepticism needed in discharging their duties. Further, as Financial Director, Ms. Sachdeva would have been the primary person who would have assisted the auditors, prepared for their visit and answered queries that they might have raised.

- Although KOSS was an SEC regulated company, due to its size, it was able to opt out of having an internal controls audit performed (under Sarbanes-Oxley) and having its auditors provide an opinion as to the company's internal controls. The person from management who provided a certification was Mr. Michael Koss himself who was not the Financial Director and therefore did not have first-hand knowledge and experience of the company's internal controls.

- The approach of the external auditors which included having the most junior member of the external audit team performed the fieldwork on bank reconciliations.

- The fact that executive management was somewhat "hands off" and that, by his own admission, Mr. Michael Koss had never reviewed the bank statements of the company.

- Risk management policy and procedures to detect and prevent such kind of fraud were completely missing as board didn't pay attention on it. What is apparent is that there was a distinct lack of corporate governance. At the minimum, Executive Management would have been expected to review the financial results of the company on the monthly or quarterly basis and have some "feel" as to what the results should be. It would appear that much of the misappropriation was disguised as cost of sales. It is surprising, that as technical experts, the executive management did not seem to have more of a handle on what their ratio between sales and cost of sales should be.

5. The Control Failures that Lead to the Fraud Not Being Detected Earlier?

The fraud went on for more than a period of 5 years with the amounts being misappropriated becoming progressively bigger. Amex contacted Mr. Michael Koss because they became suspicious that wire transfers from a company bank account were being used by Ms. Sachdeva to settle her own Amex bill. Had Amex not expressed this concern, then it is likely that the fraud may have gone on longer without being detected. In order for a fraud of this magnitude to be perpetrated over a five year period and not be detected, there must have been control weaknesses at all levels within the organization. Potential control weaknesses included:

- The lack of a budgeting system which could be monitored by executive management. Had management prepared a budgets based upon a solid understanding of expected sales, cost of sales and expenses, then unusual items might have been detected (Cohen et al., 2002). Adding to this, since there were no thoughts of budgetary control, it is unlikely that executive management reviewed the financial results on a regular basis.

- The fact that executive management did not appear to have a grip on the cost of producing goods as well as the expenses that the company was expected to incur. The fact that Ms. Sachdeva was allowed to work in relative isolation with very little monitoring or oversight of her work taking place. This would have allowed her to perpetrate the fraud with minimal chance of being detected. It appears that she was able to exert influence on her colleague to pass journal entries to “hide” the amounts that had been stolen.

- The accounting department was small due to the size of the company and, therefore, there would have been a lack of segregation of duties. Management should have been aware of this and taken measures, such as internal audit outsourcing, to put alternative controls in place.

- Given the size of the company, all cheques and requests for wire transfers should have been countersigned by Michael Koss after review of supporting documentations. It does not appear as though Michael Koss was a signatory to cheques or wire transfers that were drawn on the company’s bank account.

- The fact that the bank with which KOSS had its banking relationship was probably familiar with the perpetrator in her capacity as Head of Finance of the company and therefore might not have been as vigilant as they should have been in ensuring the validity of her requests.

- The fact that the auditors had been in their position for a substantial length of time and might not have been as skeptical as would be expected of external auditors. Further, the auditors had not been asked to do an audit of Internal Controls over Financial Reporting (ICFR) under the Sarbanes-Oxley Act and therefore would not necessarily have spotted control weaknesses.

- It also could be the case that the GT placed undue reliance on controls but did not perform sufficient testing of controls. This would have limited their substantive work during

the audit process. Through performing a substantive audit, there might have had more chance of detecting the fraud.

- It appears that the company did not have any form of internal audit function since it is a relatively small company, they could have contracted for an outsourced internal audit function that could have performed internal audit on periodic basis, may be alternative year.

- The audit committee should have been more critical in examining the role of the external auditors and their performance as well as being robust in questioning the results of the company, along with the control environment. The committee should be more vigilant on fraud prone area of business.

- It does not appear as though the company had outside (independent) directors. Again, independent directors might have been more skeptical in reviewing the results and there would have been a higher chance that they would have questioned the controls environment and set right tone at the top.

6. How the Fraud Was Detected? What Was the Role of Auditors and Why They Were Unable to Detect the Fraud on a Timely Basis?

It appears that the fraud may have continued for a longer period. Was it not for the vigilance of Amex? Amex became suspicious that Sachdeva's personal bills were being settled from the KOSS corporate account and contacted Michael Koss, CEO. This leads to the fraud being uncovered. After it came to notice of Michael, it was reported to SEC and further investigations were started.

The role of auditors was to do careful audit, follow all PCAOB auditing standards and express their opinion based on the evidence and audit procedures. It seems they may have failed to do so. GT always issued an unqualified opinion on financial statements to KOSS. Initially, GT refused to accept the blame for negligence and claimed that preparation and fair presentation of financial statements as well as designing the internal controls are the responsibility of management. Further, they claimed that they were not assigned for ICFR audit. Because of its size, KOSS hasn't been required to have its outside auditor assess the effectiveness of the company's internal controls over its financial reporting. But later on, they admitted their mistakes and negligence and settle compensation worth $ 8.5 million. Based upon an analysis of what happened the fact that the fraud was not detected until a substantial amount had been misappropriated was clearly due to senior management not discharging their duties properly.

As much as it would be desirable (and in some cases expected) for audits to uncover fraud (and it is often assumed that audits are designed to do this), audits are not designed to uncover fraud. Financial statement audits rarely detect fraud because detecting fraud is not the purpose of a financial statement audit. If companies need to engage someone to detect fraud, then they need to hire forensic accountants specifically to perform tests aimed at detecting and preventing fraud. They simply can't rely on the auditors. Some parties are of the opinion that auditors should change their work in order to detect more fraud. But as mentioned earlier, this is not the purpose of a financial statement audit. Auditors are engaged

to audit and express a professional and independent opinion on financial statements. They are not engaged to detect fraud. The responsibility to detect fraud lies with the companies and their management, and if management wishes to detect fraud, they need to take measures over and above the standard financial statement audit.

7. Alleged Failure of GT to Conduct the Audit in Accordance with PCAOB

The following section deals with alleged failures by GT to discharge their obligations in conducting the audit in accordance with Generally Accepted Audit Standards and the requirements of the PCAOB. On July 7, 2005 GT (defendant) issued its unqualified audit report and opinion evaluating the financial position of KOSS and its subsidiaries as of June 30, 2004 and 2005. KOSS incorporated GT's audit report and opinion into is Form 10-K Annual Report, with GT's consent, and filed it with the SEC for the fiscal year ended June 30, 2005. It is contended by KOSS that the report recklessly and/or falsely stated. Each subsequent 10-K annual report filed by KOSS during the Class Period incorporated a substantially similar audit report and opinion from GT. Each of GT's incorporated reports was alleged to be recklessly false. Additionally, defendant GT represented throughout the Class Period that it performed its audit engagements with KOSS in accordance with GAAS and PCAOB standards. These representations were alleged to be recklessly false because at least the following GAAS general, field work and reporting standards were allegedly violated:

a) General Standard 3 was not fully followed, in that due professional care was allegedly not exercised in the performance of the audit and the preparation of the report.

b) Field Work Standard 1 was allegedly violated as, among other things, GT failed to adequately plan its 2005 through 2009 audits of KOSS to design procedures to detect the existence of material misstatements in the financial statements caused by error or fraud. GT failed to test the controls of KOSS which lead to wrong selection of audit procedures.

c) Field Work Standard 2 was allegedly violated in that an insufficient understanding of the client, its environment and its internal control systems was obtained, to plan the audit and determine the nature, timing and extent of tests to be performed.

d) Field Work Standard 3 was allegedly violated since GT allegedly gathered insufficient and unreliable evidence primarily from head of finance through inspection, observation, inquiries, and confirmations to afford a reasonable basis for an opinion.

e) Reporting Standard 1 was allegedly violated since GT stated that the audited or reviewed financial statements of KOSS issued during the Class Period were presented in accordance with GAAP, which was alleged not to be true.

f) Reporting Standard 3 was allegedly not complied with since there were inadequate informative disclosures and material misstatements contained in the financial statements.

g) Reporting Standard 4 was allegedly violated as GT had an insufficient basis for expressing an unqualified opinion on KOSS's audited financial statements, as its audits were alleged not to have been conducted in accordance with PCAOB standards and the Company's financial

statements were not prepared in accordance with GAAP.

8. KOSS' Violation of GAAP Rules in Its Financial Statement Filed with SEC

The financial results were cooked and misleading, as such financial information was not prepared in accordance with GAAP, nor was the financial information a fair presentation of the Company's operations due to the Company's improper accounting in violation of GAAP rules.

Regulation S-X states that financial statements filed with the SEC which are not prepared in compliance with GAAP are presumed to be misleading and inaccurate. Regulation S-X requires that interim financial statements must also comply with GAAP, with the exception that interim financial statements need not include disclosure which would duplicate disclosures in accompanying annual financial statements.

The fact that KOSS has announced that it plans to restate its financial statements and informed investors that these financial statements should not be relied upon is an admission that they were false and misleading when originally issued.

Given these accounting irregularities, the Company announced financial results that were in violation of GAAP and the following principles:

1) The principle that "interim financial reporting should be based upon the same accounting principles and practices used to prepare annual financial statements" was violated (APB No. 28, 10).

2) The principle that "financial reporting should provide information that is useful to present to potential investors and creditors and other users in making rational investment, credit, and similar decisions" was violated (FASB Statement of Concepts No. 1, 34).

3) The principle that "financial reporting should provide information about the economic resources of an enterprise, the claims to those resources, and effects of transactions, events, and circumstances that change resources and claims to those resources" was violated (FASB Statement of Concepts No. 1, 40).

4) The principle that "financial reporting should provide information about an enterprise's financial performance during a period" was violated (FASB Statement of Concepts No. 1, 42).

9. Aftermath

- The company restated its financials, dismissed its auditing firm, and changed several procedures in the finance department, including doing away with petty cash.
- It also hired a new CFO and has pledged to keep the CEO and CFO roles separate.
- Both accountants were also terminated because they failed to report the unauthorized transactions to top management or the audit committee. Both accountants have been charged by the SEC with Sachdeva receiving several criminal charges and Mulvaney being charged with civil fraud.

- KOSS has hired Baker Tilly Virchow Krause as its new auditors, and this firm will not only do future audits, but will also audit any prior period financial statements that need to be restated.

- Ms. Sachdeva could face a maximum penalty of 120 years in prison and fines of up to $1.5 million as well as being required to pay back the misappropriated funds.

- KOSS has now acquired the unwelcome reputation as providing an excellent case study of how important a robust system of internal controls and a proper ethics and code of conduct are needed, no matter what the size of the company.

10. What Can Be Learnt from this Fraud

This fraud holds several lessons for smaller companies and how they are managed, controlled and regulated. The fraud at KOSS was allegedly committed over a five-year period worth $34 million and incredibly, continued for much longer than five years if Amex not informed KOSS's CEO about two large wire transfers made from its company account to Sachdeva's personal credit card. Sachdeva allegedly did her best to hide the wire transfers by falsifying the bank balance and manipulating cost of produced goods.

So, at a first glance, it looks second- generation family management business defrauded, along with passive investors. But, some other experts might look it differently. The headline of a CFO.com article, "Fraud Case Feeds Sarbox-Exemption Critics" implies that if smaller companies had not been exempted from ICFR audit, frauds of such kind could be detected earlier.

Despite its modest size, there are lessons that can be learnt from the KOSS fraud; but these lessons are not that smaller reporting companies should have to obtain an audit of their ICFR. The lesson is more like, 'simple problems have simple solutions.' The reasons are as follows: (1) The first lesson is related to the costs and benefits of the ICFR audit. These have been discussed extensively and it is inferred from many researches that this type of audit would not have significant benefit to smaller companies, particularly in preventing fraud. (2) The board of directors has a fiduciary duty to shareholders to ensure that the company is led by capable executives who are aiming to achieve appropriate business objectives. The first thing for board is to be evaluating planning and budgeting processes of the company. Indeed, it would be surprising if board did setting sales goals only. But, if KOSS had a careful profit planning, and the discipline to rigorously evaluate variance periodically against that plan, the unauthorized expenditures would have become uncovered. An audit of key ICFR would be of no benefit in correcting the above.

Under the Sarbanes Oxley Act, the Chief Executive Officer and the Chief Financial officer are required to issue a formal statement that includes the following: to the best of their knowledge and after review of the financial statements, the financial statements are free of material error. In the case of Koss, Sachdeva did not hold the title of Chief Financial Officer but was referred to as "Vice President of Finance and Secretary". Michael Koss had the titles of "President, Chief Operating Officer and Chief Financial Officer". He had held these titles for more than 20 years and, by default, signed off the Sarbanes-Oxley statement in the dual

capacity of CEO and CFO. The authors assume that the dual sign-off on the SOX certifications had been approved by KOSS's lawyers. If this was the case, their interpretation of the provisions of the Sarbanes-Oxley act and SEC regulations was at best, liberal.

It is difficult to understand how Michael Koss signed off the SOX certification in a capacity of CFO when his knowledge of the company's detailed finances was clearly lacking. At the risk of stating the obvious, the person who should have signed off the SOX certification should have been Sachdeva, who was the only other named executive with a finance related title disclosed in the senior management compensation disclosures.

It is clear that the SEC should provide more guidance as to when a person can sign off the SOX certification in the dual capacities of CFO and CEO. This should certainly be the exception rather than the rule and it would be expected, that in order to do this sign-off, an issuer should seek a dispensation or exception from the SEC.

Securities lawyers tend to recommend that their clients disclose the minimum required by the SEC and no more. An Internal Controls audit would not have addressed this issue but better advice could have been given by the securities lawyer. Notwithstanding anything that GT has announced to the public in its own defense, it is difficult to understand how GT could have missed a bank balance that was falsified to the extent the KOSS's was?

For legal reasons, there has not been a large amount of information disclosed regarding the audit process and why the fraud was not detected. However, we do know that the fraud was perpetuated over a period of five years, and hence, five audit cycles.

It is surprising that the auditors did not query the large transfers to Amex (who were not a regular vendor) of $382,000 and $1.4 million. These amounts would certainly be considered to be material in a rigorous audit process and therefore, should have been subject to greater scrutiny by the auditors.

KOSS's audit committee was composed of who were considered to be "independent". Further, the board members had unfettered access to its own outside experts, and were meant to oversee the work of the auditors. Three of the four members of KOSS's audit committee had been serving on the board for more than twenty years. This is a lengthy period and not considered to be good practice as these members would have become overly familiar with the company, and hence may have lacked professional skepticism. Further, none of the members had any significant accounting or auditing experience, which is also not considered to be good practice. The audit committee "financial expert" at that time was, and remains, John Mattson who has been retired for some time. The only credential that appeared to be relevant to his role on the audit committee was that he was a retired president of Oster, a division of Sunbeam Corporation.

Given the apparent attitude of the Board and Owner of Koss, it would have been easy for an audit of the internal controls over financial reporting to become a mere compliance exercise. In particular, given the composition of the Board and Audit Committee their knowledge may have been outdated and they may have placed unwarranted reliance on the auditors and the audit process (including the ICFR audit). The SEC and its analysts are meant to review the

financial statements and other submissions related to the companies that they regulate. It is surprising that a fraud involving loss of around 20% of the company's turnover for a period of five years was not detected by the analysts. Any analyst (or external auditor) would have queried the financial statements if a reconciliation of the opening and closing balances of the balance sheet accounts was a required disclosure in the notes to the financial statements. It would have been extremely difficult to hide the misappropriation of such a significant amount of funds.

An ICFR audit does not replace the need for robust external controls to be in place over financial reporting. If it is the aim of the SEC to gain a significant improvement in the quality of financial reporting through adopting elements of IFRS, the SEC needs to clearly state to Boards and Audit Committees that they require full disclosure and transparency related to changes to balance sheet accounts. This would be a highly effective measure in discouraging fraud and "earnings management".

In summary, simply identifying and strengthening elements of internal control systems that are already in place would arguably be more effective than an ICFR audit (COSO Report, 1992). The following should be adopted:

- Transparency should be increased through detailed reconciliations of balance sheet accounts.
- Mandatory audit firm rotation should be put in place to strengthen auditor independence.
- The independence of Boards and Audit Committees should be enhanced through more detailed disclosure requirements and regulatory oversight.

These practical recommendations, either singly or combined are recommended prior to considering imposing ICFR audits on smaller SEC regulated companies.

Otherwise, an ICFR could be mandatory every 3 or 4 years.

In the case of KOSS, it appears that Sachdeva was a highly trusted employee. She had been with the company for 17 years, and was likely given a lot of autonomy in her function as the head of the company's finance team. Too much autonomy is dangerous for an executive at any company. Checks and balances (or "internal controls") need to be inplace so that other executives and the board of directors are involved in the accounting function on some level. If there had been greater oversight, it's likely that any alleged fraud would have been uncovered much sooner (Kroll et al., 2008).

11. Limitations of This Study

This case study is prepared, for educational purposes, based on public available sources such as newspapers, magazines, websites and other referred articles. The primary objective of this case study has been to bring together a good summary of the enormous amount of public domain information that is available on this case. As mentioned above, all the information used is available in public domain and authors have no access to inside information. Further, some of the opinions expressed are those of the authors and cannot be represented as the

views of anyone else. Where the views of others are expressed, these are referenced. Both authors never worked as auditors or in other capacities with KOSS and they never hold investments in shares of KOSS. The authors have not interviewed any parties that have been involved in the management of Koss, the audit of Koss or the investigation of the fraud.

References

Brenner, S. W. (2001). Is There Such a Thing as "Virtual Crime"? *California Criminal Law Review, 4.*

Chapman, A., & Smith, R. G. (2001). Controlling Financial Services Fraud. *Trends and Issues in Crime and Criminal Justice*, No. 189. Australian Institute of Criminology, Canberra.

Coenen, T. (2010). Anatomy of an Alleged $31 Million Fraud. [Online] Available: http://www.dailyfinance.com/2010/01/18/koss-corp-anatomy-of-an-alleged-31-million-fraud

Cohen, J., Krisnamoorthy, G., & Wright, A. M. (2002). Corporate Governance and the Audit Process. *Contemporary Accounting Research*, *19*(4), 573-594. http://dx.doi.org/10.1506/983M-EPXG-4Y0R-J9YK

Curtis, V. C. (2011). How an embezzler stole millions from a small company. *Strategic Finance*. [Online] Available: http://www.accountingweb.com/aa/law-and-enforcement/how-an-embezzler-stole-millions-from-a-small-company

Grabosky, P., Smith, R. G., & Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in Cyberspace*. Cambridge: Cambridge University Press.

Greenspan, A. (2002). Monetary Policy Report to the Congress. *Federal Reserve Bulletin*, July 16.

Johnson, S. (2010). Fraud Case Feeds Sarbox-Exemption Critics. [Online] Available: http://ww2.cfo.com/accounting- tax/2010/01/fraud-case-feeds-sarbox-exemption-critics

Koss. (2010). (Press Release). [Online] Available: http://investors.koss.com/releasedetail.cfm?ReleaseID=654455

Kroll, M., Walters, B. A., & Wright, P. (2008). Board vigilance, director experience, and corporate outcomes. *Strategic Management Journal*, *29*(4), 363-382. http://dx.doi.org/10.1002/smj.649

Lanham, D., Weinberg, M., Brown, K. E., & Ryan, G. W. (1987). *Criminal fraud*. Sydney: The Law Book Company Limited.

Mile, S. (2007). Committee of Sponsoring Organizations of the Treadway Commission Internal Control - Integrated Fromework. *Revizor*. New York, NY: COSO Report.

Parker, B. D. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Willey & Sons, Inc.

Rebovich, D. J., & Kane, J. L. (2002). An eye for an eye in the electronic age: Gauging public

attitude toward white collar crime and punishment. *Journal of Economic Crime Management, 1*(2).

Smedinghoff, T. J. (1996). *Online Law, The SPA's Legal Guide to Doing Business on the Internet*. New Jersey: Addison-Wesley Developers Press.

Smith, R. G. (2001). Defining, Measuring, and Reporting Fraud Risk within Your Organisation. Applying Risk Management to Implement a Proactive Fraud Prevention Strategy in Financial Services, I.I.R. Conferences, Parkroyal Darling Harbour, 19-20 July 2001. [Online] Available: http://www.aic.gov.au/conferences/other/smith_russell/2001-07-IIR.pdf

Veneziani, V. (2010). How To Steal $31 Million From Your Company, Go On A Luxury Shopping Spree, And Nearly Bankrupt Your Firm. *Business Insider*. [Online] Available: http://www.businessinsider.com/meet-the-woman-who-stole-31-million-from-koss-corp-2010-1

Copyright Disclaimer