Accounting crime and fraud challenges

When I was in prison, visiting, an inmate came right after my presentation and said "Mustapha I really appreciate your talk on in-mate reformation. But how do you advise someone like me serving a jail term for a crime I never committed?"

This was my first face to face with a victim of fraud, 10 years ago. Then an Accounts Officer at a local NGO, the victim was serving a jail term for misappropriation of petty cash. He was a young accountant on his first job. He explained to me that he had been requested by his supervisor, the Finance Manager, to raise petty cash vourcher, sign them and release cash from the float.

Oblivious of the future accountability challenges for the funds in his possession, the young man cared more about the nods and smiles from his boss until an impromptu audit of the funds at the request of the donor suddenly opened the Pandora's Box. The timing was so bad that it came at a time this particular NGO's new leadership wanted to make a point: no money is too small. The case became of interest to those concerned and prosecution was delivered against the young accountant or the young man doing the role of the accountant. As his boss went smiling to the bar, the young man headed to that special University of Understanding.

That is economic crime and fraud for you. Very pervasive. The externalities of a single incident are so much that you are a suspect until facts and evidence prove otherwise. And most of the time, the evidence may point to folks who were excited to execute their new responsibilities.

As the key player in the overall health of the business, Accountants are at the center of accountability and preserving stakeholder value at all times. The increasing ingenuity of fraudsters means that accountants too must keep upping their skills to proactively prevent fraud schemes that come in so many shapes and colors. Let's take a look at some I have been at the center of investigating.

Nigerians are known for their 913 Internet schemes that have been around since the early days of the Internet. It is unfortunate that some people, educated ones of the Accountant's ilk at that, still fall for such schemes. Many of these nowadays come in the form of travelling abroad for a conference at a University with a promise to get a higher degree after five days of study. The ambitious ones will promise you an award to your entity for outstanding leadership as nominated and evaluated by the fraudsters purportedly based in Brussels or some European city. If you have a website, you have probably witnessed such kind of malfeasance. The amounts involved are insane. But that is ok. You are the victim and at least you get the opportunity to travel at the expense of your employer.

A local organisation engaged an IT company for computer maintenance services. A service level agreement (SLA) was signed, specifying clear terms and responsibilities for each party. During the course of the work, unknown to the client, the IT Company outsourced part of the work to an external vendor who during execution, discovered the nature of transactions of the organisation. Specifically, the organisation made payments for specific imported products purchased from specific companies in the US and Europe. Using free Internet tools, the suspect (external vendor) copied the entire website of the US supplier and made the replica look exactly like the genuine one and also advertised all the products the company sells. He then sent a link to the victim organisation via a cloud (anonymous) email address, who unknowingly placed orders through the rogue website. In the process, payment instructions were exchanged. The first was a bidding security payment of US $90,000. Thereafter, the victim was further asked to pay US $250,000 as part of down payment to facilitate shipping and delivery, among others. Before the goods could be shipped, the victim organisation was further asked to make more payments, which aroused the Chief Finance Officer's suspicions. The genuine company never asked for these kinds of deposit payments over and above the bid security, though at first they had thought of it as a change of process. Most frauds involve collusion, the victim organisation would have been sucked dry had the CFO been

Research by the Association of Certified Fraud Examiners (ACFE) contained in the 2017 Report to The Nations (RTTN) states that an average organisation loses about 5% of her annual revenue to fraud.

in the loop of the scheme. It came to pass that the CFO's doubts were genuine.

And that is what makes most frauds and such economic crimes a challenge – when the people entrusted to protect company assets fail to uphold the profession's codes of conduct in all of their dealings, by applying the fundamental Accountancy ethical principles of honesty, integrity, objectivity, independence, commitment to professional competence, due care, and confidentiality. There is nothing as painful as looking a fellow professional in the eyes and holding them accountable for resources under their control.

Though the above case may not be a direct accounting crime, it is a fraud that is very sophisticated as it of cyber in nature. Indeed cybercrime is on the rise and there is probably no fraud or crime that can be committed in this era without the use of computers or digital devices like mobile phones and the Internet in committing it. That is the challenge which today's accountants find themselves facing: how do you preserve and grow shareholders value amid so many fraudsters with an arsenal of attack vectors and weaponry that are unpredictable?

Over 70% of most Ministries, Directorates and Agencies (MDAs) of Government and other entities main business is spending on a budget. Ministry of Finance will apportion and disburse the funds from the consolidated fund. The MDA will just spend it. The same applies to NGOs.

It goes without saying that most finance departments spend a lot of their time managing expenditures and overseeing procurement. The devil lags in there. From bribes (a staff involved in procurement receives a thing of value to influence a pending decision to award a deal), to kick back (a token of appreciation going back to the procurement staff), from leaking confidential data of competitors to a favored bidder to give undue advantage, to bid manipulations (maneuvers to favour a bidder to change bids or specifications), the list is endless. Many cases abound where delivery of the contract is deliberately delayed as costs are incurred. The end result is a bidder receiving higher pay for no work done as a result of contract frustration by the client. The common denominator is all these is collusion. Is today's accountant beyond reproach?

Research by the Association of Certified Fraud Examiners (ACFE) contained in the 2017 Report to The Nations (RTTN) states that an average organisation loses about 5% of her annual revenue to fraud. That is a lot of money. Every organisation is losing money to fraud: the question is how much? The challenge with fraud is that few organizations have mechanisms or systems to detect and ascertain the actual extent of the loss. By far, asset misappropriation tops the pack.

Enter Crane Bank.

A couple of years back, Crane Bank Limited was a phenomenal affiliate of the Ugandan economy. It was clearly a model bank. Had established branches countrywide and instilled a brand almost every citizen knew about. However, a few years later, the European Investment Bank (EIB) saved it by refueling with money in 2014 and the Bank consequently published record results in 2015.

Astonishingly, by 2016, Crane Bank was suddenly under heavy losses. This took most of the public aback. But a few signs had been evident. Their accounts weren't as clearly as they had stated. Some analysts suspected a connection of this fiasco on the notorious #ScamBaillouts of companies that had very many accounts at the bank. A customer base of almost 500,000 customers was muddled. BoU subjected Crane Bank's paid up capital to a forensic audit which exposed the bank's shenanigans.

At least 1 in 5 internally perpetrated frauds still involve senior management, though the majority of such frauds tends to be committed by junior staff or middle management. The Central bank reported that the owner of the bank, Mr. Sudhir Ruparelia (senior management) and his Meera Investments had swindled the then Crane Bank of billions of shillings in fraudulent transactions and invoices. According to BoU, he had fraudulently transferred the bank's assets into his personal ownership. He would also lend himself from the bank's capital and later write off the debts as bad loans – something

that sounds accounting crime. More so, Ugx. 334bn and another Ugx. 8.2bn of depositor's money is reported to have been taken out for personal gain. The questions on everyone's lips have been: where were the auditors? Of course the accountants are inside there hiding. When will they come out? No one knows. So, how can a director commit an accounting crime without the knowledge of the accountant or chief finance officer at the center of balancing the books, providing strategic information with facts and figures on the financial performance and position of the bank? The more these questions are asked, the more you miss it.

And so the Bank of Uganda Governor came out to clarify that fraud by its nature is hidden. And no supervisory mechanisms can uncover some frauds as was the case with Crane Bank. And that exactly, is the accounting crime and fraud challenge: it is not easy to detect. The revelations by the Governor are an eye opener. Could other banks be losing money under our nose?

Given the nature of fraud and they psychology of fraudsters, it is a vice that will always be present. It is like to proverbial taxes, death and prostitution. The latter two are as old as mankind. And taxes are discoveries by man to rule over him completely. To this end, research points to an effective whistleblowing regime as anti-dote to fraud. A good anonymous whistleblowing system, that provides 99% anonymity like the one implemented by the National Social Security Fund, https://nssf.julisha.org is recommended as it puts doubt in the minds of the parties intending to collude that the other person could report them. That could be the only thing to save the organisation that life blood it needs to thrive.

As a fraud examiner, I have had a good share of escapades. Investigating accounting crimes is not an easy thing. Others have branded us cowards. But how do you explain a scenario where you are driving heading to town. As you wait in the traffic holdup at Jinja Road traffic lights, a middle aged man, in a dark suit, comes close to the driver's seat. Bend over to you via the window and making clear you look at his Pistol in the inside pocket politely asks you to go slow on the fraud you are investigating. And advises that "I would appreciate if you reported that your computer was stolen and all files lost. Otherwise, I would not want to come to your home to pick them personally."

Such is what was visited to yours truly once during one of such snooping around. They say talk is cheap. But what if someone does it in day light in the city center and just gives you the opportunity to think about it. In 2014, over Euro 540,000 was wired from a global institution's account in a European bank to several accounts in over eight different local banks in Uganda in ranges of Euro 76,000. The accounts had been opened in the names of two ladies with an address of Mbarara.

These ladies using fake identities succeeded in withdrawing over Euro 455,000 from about six banks. And then I was asked to investigate in which we tried to freeze the accounts, rather late but on two. It was surprising that no proper KYC had been done on these ladies. And they had withdrawn huge sums of money over the counter from accounts that had no record of business activity and walked out of the bank just like that. As an investigator, when you go after such fraudsters, you must make sure that you have a very huge state machinery behind your back or your insurer is prepared to take care of your family.

That, my friend, is the challenge of accounting crime. The fraudsters know they will not be caught. And if attempt is made, they will find their way out of the mess. And if prosecuted, the evidence will not be sufficient. They will fight back against the organisation. The latter happened to MTN. In 2015, the Anti-Corruption Court heard a major mobile money fraud against six ex-employees of MTN charged with defrauding the company of 10 billion UGX (US$3.4 million). Among those charged were MTN's former Finance Manager, along with the Head of Public Access and mobile money, who then counter-sued MTN for wrongful dismissal. That is fraud for you. The hunter becomes the hunted. And it not surprising that most fraud cases in the financial sector never enter the houses of justices.

The only way to overcome fraud challenges is awareness and integrity. May you think more about your conscience and not self-aggrandizement? There is no price for peace of mind.

CPA Mustapha B Mugisa works at Summit Consulting Ltd as a strategy and risk expert, which include fraud and forensic investigations and cyber security services. *Visit www.mustaphamugisa.com or email pentest@summitcl.com*