International Fraud Awareness Week

15 - 21 November 2020

ACFE Mumbai Chapter and EY Forensic & Integrity Services

The COVID-19 pandemic has businesses experiencing testing times like never before, while significantly accelerating digital transformation. With the economy gradually opening and the government and companies reinvesting in people and businesses, organizations are likely to continue facing many unfamiliar challenges in the areas of fraud detection and prevention.

Fraud and white collar crime have surged, making efficient and effective risk and compliance management even more crucial. For example, appointing new third-parties – suppliers and vendors without proper due diligence or opening firewalls for work-from-home access to company systems and tools has led to a plethora of risks. There is a constantly evolving landscape of frauds being committed by those seeking to take advantage of the anxiety and uncertainty that the pandemic has created. e-Commerce frauds, involving fake or adulterated sanitizers and cybercrimes such as phishing, malware and ransomware attacks are just some of the foothill problems created by COVID-19.

While the road to normalcy is hard to predict in such tumultuous times, organizations need to quickly adapt to the pace of change to remain resilient. Channelizing efforts for business resurgence, recovery and continuity, using technology and digital platforms, and exercising increased vigilance to address fraud risks have become a pressing priority.

Through initiatives such as International Fraud Awareness Week by the Association of Certified Fraud Examiners (ACFE), ACFE Mumbai Chapter, along with EY Forensic & Integrity Services are trying to raise awareness around the fraud risks affecting businesses. As we show our support for Fraud Week, we are pleased to share this newsletter, which captures fraud trends in 2020, viewpoints from industry leaders on their compliance and anti-fraud and corruption efforts. We would like to thank all contributors and sincerely hope you find it an interesting read.

Arpinder Singh

President and Founder, ACFE Mumbai Chapter
and Partner and Head - India and Emerging Markets,
Forensic & Integrity Services, EY

How agile forensic professionals and technology integration in risk-based frameworks can redefine the anti-fraud ecosystem

Of late, I have been seeing that there are growing opportunities coupled with a continuous and rising demand for Forensic professionals. The global recession, corporate failures, banking crises, money laundering, corporate fraud, cyber-attacks, volatile markets, disruptive innovation and other developments necessitate the need to have more of us in the system.

It is very much evident that the COVID-19 pandemic has resulted in an increase in financial crime and other misconduct due to market disruptions, reduced staff and resources, and an increase in digital uptake.

A spike in digital transactions leaves financial institutions exposed to an increased threat of cyber security and fraudulence. COVID-19 also restricts financial institutions from identifying and verifying clients; performing regulatory processes such as customer due diligence; and implementing new solutions and technology, which would typically protect organizations from these threats.

For any organization, for the Anti-Fraud Framework to be effective, the organization's executive leadership should really drive it, as what we call the Tone at the Top. Today's complex, hyper-competitive and regulated environment requires leaders to guide their organizations away from fraudulent activities. This is a simple statement and its implementation on the ground, is not as easy as it looks.

The fundamental elements of an effective anti-fraud and anti-corruption program are

- To create and maintain a culture of honesty and high ethics
- To conduct an evaluation of risks of fraud and corruption
- To ensure implementation of policies, processes, procedures and controls to mitigate such risks and reduce the opportunities for fraud and corruption
- To ensure development and functioning of an appropriate oversight process.

I see a trend and a shift in mindset on the part of regulators too, who are now more open to methods like the use of artificial intelligence (AI), machine learning and robotics. In fact, they are actively encouraging organizations to consider, evaluate and where appropriate, implement these innovative technologies. This trend does not mean we throw away the existing risk-based approach. What I see is co-existence i.e. a mixture of the existing scenarios and the AI mechanisms.

If one must call out a specific skill that all Forensic professionals must possess in abundance, then that would be **AGILITY**. The dictionary meaning of agility is quick and well-coordinated in movement. The synonyms are cleverness, dexterity, quickness, sharpness, swiftness, briskness, promptness and sprightliness which are opposed to antonyms which are slowing, slowness, sluggishness, clumsiness and stiffness.

An Agile Forensic professional is the one who focuses on stakeholder needs, accelerates review cycles, drives timely insights, reduces wasted effort and generates less paper documentation.

So, my very dear fellow professionals, let us focus on agility which will help us to adopt technology, be an integral part of strategy, develop the confidence of management and do everything that is lawfully expected of us. While we are doing it, we should enjoy the process.

Enjoy the Forensic journey, not just the destination.

Satish Shenoy

Senior President - Corporate Management Audit,
Aditya Birla Group

Fraud Talk Podcast

Fraud Talk is the ACFE's monthly podcast. In these sessions, we break down case studies, talk with the industry's leading experts and give you more tools to spot, fight and prevent fraud.

In this episode, Arpinder Singh, CFE, partner and head of India and emerging markets, Forensic & Integrity Services at EY, highlights how cybercrimes like BEC scams, phishing and account takeover have risen and will continue to rise over the next year.

The Rise of Cybercrime During COVID-19

In the News: Forensic Accounting and Investigation Standards

The Institute of Chartered Accountants in India (ICAI) announced the Forensic Accounting and Investigation Standards in September 2020. Today, there is a need for these standards due to increased cases of bank frauds, financial misrepresentation, fund diversions, as well as greater alignment with regulatory bodies such as the SFIO, SEBI, CAG etc. These will also help tiding over the absence of consistent quality in conducting investigations and lack of standardized forensic reports.

Overseen by the Digital Accounting and Assurance Board (DAAB), the Forensic Accounting and Investigation Standards will be the first set of standards exclusively for forensic accounting in India. It is expected to be mandatory for the forensic professionals, and non-adherence would be likely to invite disciplinary action. There are 30 standards under six groups.

Impact of the Forensic Accounting and Investigation Standards

- Useful to the law enforcement agencies, corporate, banks and other stakeholders
- Highest degree of professional standards in investigations
- Contribution as ‘Experts’ in Judicial proceedings
- Responsibility on the signing individual than the whole firm

Ethics in the era of digitalization

Digitalization is one of the global megatrends, and with the ever-growing adoption of digital technologies and digital applications, it has become almost omnipresent. An increasing number of corporates across sectors are in the midst of digital transformation, which is a crucial component of their business strategies. As per reports, by 2025, the global volume of data will soar to 163 zettabytes and by 2020, 30 billion devices will be connected. Nearly 80% of corporates reported to have a digital initiative under way while close to 70% believed that they need to invest in a digital strategy to remain competitive.

As digitalization disrupts society and business models, it poses both a challenge and an opportunity for Compliance Officers. More than ever, this transformation makes a convincing argument for laying stress on the importance of business ethics in the functioning of any company. A corporate must essentially develop a character for the company rather than only stress on more processes since it is the character with which the company gets identified in the long run.

Why? Consider the amount of data, growing at an exponential pace, available for corporates to harness. Combine this with the emergence of powerful technologies such as machine learning and artificial intelligence. New skills have also materialized, such as data mining, data visualization and risk analytics.

It is in such a scenario that new risk management techniques and strategies need to take shape. Corporates, with a strong ethical character, will effectively combine the need for reviewing processes, making tools intelligent and automating risk identification with role models for good corporate governance among senior management.

For every corporate, the journey for achieving good corporate governance commences at the very top. As culture starts at the top, it is very important to have the right members as role models and captains of the businesses. Healthy debates, quality of discussions, allowing dissent in a healthy manner within the management teams are all essential and vital. ‘Walk the Talk’ by the management sets the tone for values within the organization, not just maximizing efficiency, monitoring business processes and automating compliance controls.

It is only values that can lead to sustainable business. Leadership guru Peter Drucker said, ‘Culture Eats Strategy for Lunch’. Hence, a lack of speak up culture would not be able to sustain an organization.

‘Speak up culture’ should be encouraged and all employees should be encouraged in ‘speaking the truth; being honest and trying to build a value-based organization’ as this is what creates a good ecosystem for good corporate governance. Such an organization is bound to succeed over the long term in the digital age, where the constant focus on quality, flexibility and efficiency forces constant change upon employees!

Building a robust moral fabric is important as only that would lead to sustainable and profitable business.

The Indian industry has taken to digitalization, with some sectors being able to identify and exploit the benefits earlier than others. From an Indian perspective though, there still exists a trust deficit between government, industry and society. The basic reason behind the widening gap is the question of ethics and how each pillar could try to ensure ethical behavior, specially at a time with digitalization also brings in transparency and speed!

As the Indian Industry has so far seen six committees formed to educate and direct industry on what constitutes good ‘Corporate Governance’, its importance could not be better underlined.

Due to some misdemeanor by industry the government promulgates new regulations, which demand increased disclosure requirements by corporates while on the other hand the industry looks up to these committees to guide the industry captains on good governance. It is an oxymoron that needs quick addressal.

Deliberations within organizations that have been found wanting in compliance have revolved around the question of what was more essential and important: Having more processes or developing a character for the company?

Values can never change with technology or newer business models. To sum up, building up of moral fabric is very important as only that would lead to sustainable and profitable business.

Neville K Gandhi

Vice-President Compliance, Siemens Limited

What do we do at Schindler India to prevent fraud?

The Schindler compliance program reflects a strong commitment by Schindler employees to live the Schindler values, every day. We have a Code of Conduct policy, which all good companies have, and it is extended to our vendors and intermediaries. To implement the same effectively, in day-to-day business, we rigorously follow the three “E’s” formula - **Educate, Examine & Enforce**.

Educate

The beauty of the Schindler **Code of Conduct (CoC) Policy** is that it’s a one pager document with five principles. Simple to understand, co-relate and follow. The compliance department devotes its maximum time on training and ensuring all the activities are under training rigorously. The activities under this "E" are:

Explain the CoC at the time of induction and then ensuring that each employee undergoes personal training minimum once a year. The CoC is always item no.2 in all the management meetings, first being **Safety**. During COVID-19 times also the process of training is effectively conducted, with a change in model of virtual training, but keeping it interactive. Records of attendance are collected and kept on file. We started this year a new initiative of monthly **CoC newsletters**, which is a one pager circulated over email to all the employees.

Besides this, we also run a **Compliance Radar**, where each employee is given the opportunity to speak up and voice any compliance risks. This is in addition to a hotline whistleblower process, which is also in place.

Each employee undergoes **eLearning** once a year and has to clear the exam, with passing percentage being more than 80%. All new joiners have to pass eLearning during their probation period and it’s one of the conditions for confirmation.

We also have a direct hot line for whistleblowing and disclosures, which is open 24/7. The code of conduct policy is an integral part of vendor and supplier agreements, and it is one of the conditions for forthwith termination, in case of violations. We run a due diligence process on major vendors and suppliers.

Examine

The data of the trainings and other activities are self-audited and undergo a third person audit, done by another Schindler group officer. The gaps and opportunities for improvement, if any, are discussed and process goes on.

We have several examine processes: monthly expense audits, with CoC perspective, compliance clearances for processes with elevated risks, spot checks, data analytics etc. We follow examine principle of effective implementation, in a fair mode and the results are discussed at senior management level.

Enforce

The violations, if any, are taken seriously. Proper impartial investigations are conducted by independent compliance officers. Fair treatment, including right to be heard, is offered to alleged perpetrators. A deep dive is conducted to find out motives and rationale.

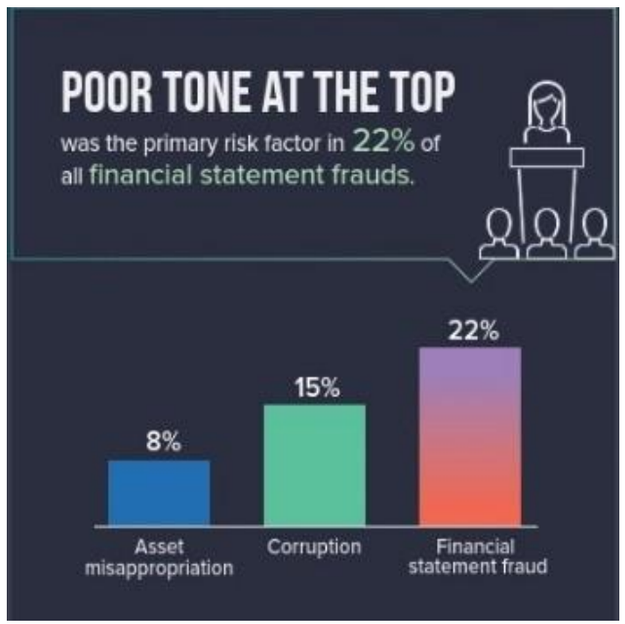
In a continuous learning process, violation practices are reviewed, and risk control measures are improved. Accordingly, we have various Risk Control modules in place, to avoid and mitigate the various types of fraud. We not only impose sanctions, including termination, for violations; we also extend rewards and congratulations for doing the right thing. We cover and circulate learnings in our future training materials.

Atul Juvle

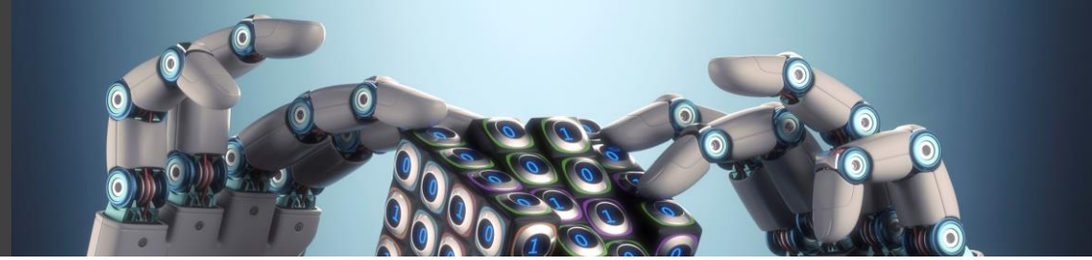
LL.B., F.C.S. M.F.M., CFE

General Counsel, Compliance Officer & C.S, India & SA, Schindler

The report covers recent trends on how occupational fraud imposes tremendous costs upon businesses and government agencies throughout the world.



Evolving fraud techniques in 2020



The COVID-19 crisis has introduced us to the “New Normal” world of high usage of Digitalization and Artificial Intelligence. Most business transactions globally are taking place online with high value of digital accounts. Fraudsters and cybercriminals have been taking utmost advantage of this situation. Some aggressively evolving fraud techniques in 2020 are listed below:

Account Takeover (ATO)

This technique is used to steal login credentials of individuals as well as organizations. High net individuals and big corporates are the main targets for these kinds of fraudulent activities. Organizations have created IT firewalls to mitigate this risk, so that these ATOs cannot be successfully commissioned. Our organization has a full-fledged IT Shared Business Services Centre which is equipped to combat these kinds of frauds.

Phishing

Organizations and individuals have been widely losing valuable assets without giving away passwords. This tactic allows attackers to access data stored in the cloud by directing them to the real login page via a malicious link.

Those who take the bait end up forwarding a digital token which gives fraudsters indefinite access to all the cloud data, including emails, files and contacts – even after the victim changes their passwords. Merck’s IT team has been periodically sending mails to all employees to create awareness about phishing, that they should not fall prey to these attacks and the ramifications, which could cost the organization dearly.

Money Laundering

Currently, it represents between 2 – 5% of the global GDP, or close to $800 billion to $2 trillion, according to the United Nations Office on Drugs and Crime.

The goal of money laundering is to move the cash around to create layers that obfuscate the source of the criminal funds and, ultimately, turn the proceeds of crime into "legitimate" assets.

Merck has designed a global project on Anti-Money Laundering (AML) to create awareness amongst the senior leaders worldwide and eLearning modules are rolled out to the entire organization.

Business Partner Risk Management (BPRM)

Organizations rely heavily on their business partners (BP) for improved profitability, faster time to market, competitive advantage, and decreased costs. However, BP relationships come with multiple risks that include:

BPRM is the process of identifying, assessing and controlling these and other risks presented throughout the lifecycle of relationships with BPs. Our organization is in the process of introducing an improvised, sophisticated version to the existing IT tool which will conduct due diligence of BPs more effectively and mitigate risks substantially.

Fraudulent App Installations

There's a huge number of malicious mobile apps on shopping, travel, gaming which lead to mobile frauds. Countries like Vietnam, India and Indonesia offer a perfect ecosystem of:

- Higher mobile user volumes
- High marketeer demand for volume
- High rate of fraudulent traffic in local networks
- And a trend towards a cost per action (CPA) business model.

In South East Asia, the numbers are even more shocking, due to a market driven by cost per install (CPI), which creates a strong incentive for fraudsters to use bots and multiply attacks, even with what appears to be low payouts. The good news is that anti-fraud solutions have fantastic track records in reducing bot attacks and install hijacking. So, prevention is indeed possible, if marketers leverage these solutions efficiently and fast.

Merck has taken leadership in Organizational Risk Assessment by implementing Compliance Risk reporting and Self-Monitoring tools which helps identifying and mitigating risks at the local country and company level. It's an integrated approach which helps to better manage risks in a way that builds trust, confidence, reputation and growth for the organization at large.

Deepa Bhandare

Compliance Officer – HC India & Thailand
Merck

COVID-19 – Understanding the impact using the Fraud Triangle

The COVID-19 crisis caught businesses unprepared and companies worldwide had to transform their business models quickly to adapt to the new normal. Fraudsters too were able to capitalize on the opportunities, uncertainties, fear and challenges to target organizations and their employees.

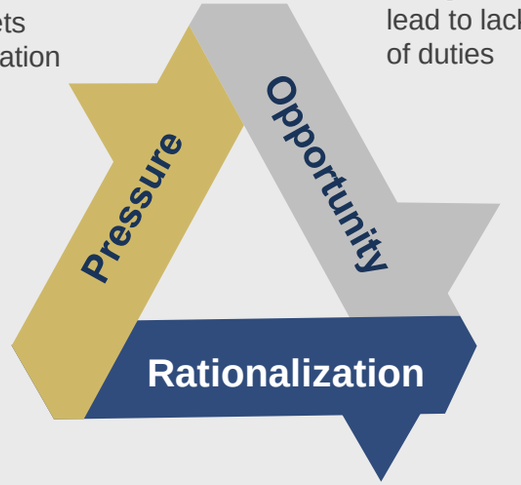
Repercussion from the crisis include pay cuts and job losses

Rising fear of retaliation may have employees failing to exercise restraint and giving into management overrides

Pressure to achieve targets may lead to misrepresentation of financial statements

Scammers are increasingly targeting unsuspecting employees through phishing, vishing, SMS-phishing and other technology led scams

There is a reduction in the number of people in charge of controls could lead to lack of segregation of duties



The unprecedented scenario may provide a "compelling" argument to justify cutting corners or misconduct

Employee perceptions, reduced monitoring or oversight may lead to unethical practices

Building an organization's strong anti-fraud culture

A culture of integrity and transparency in a company helps in creating an open work environment. Any company looking to ensure a fraud free environment needs to proactively define various initiatives and should take appropriate measures.

To make an organization's strong anti-fraud culture, there are various important aspects which are critical.

For example,

- Defining the anti-fraud policy of the company and effectively publishing it for its better reach
- Defining the expectations of the company from each of its employees which may include the conduct from its employees, the expected values to be followed while performing any of the duties, etc
- The awareness among the employees as to how each one can contribute in achieving a fraud free work environment
- Setting the tone of the organization by ensuring a zero-tolerance approach toward any breach to the anti- fraud policy
- Publishing the incident reporting structure at all levels for ensuring timely reporting of any type of fraud at any level. This involves mechanism like advertising the hotline numbers and email addresses on which fraud cases can be reported by anyone.
- Regular conduct of trainings, awareness and campaigns of the defined anti-fraud policy for better assimilation and complete familiarity with the policy

After taking all the precautionary steps as stated above, it is equally important to define the penalty and disciplinary actions which can be taken by the management or a defined committee.

While interacting, conducting trainings, awareness sessions, campaigns and investigation of the reported cases, the learning should be incorporated for continual improvement of the defined policy and to make sure that it stands current at all times.

There are various ways available presently and also emerging on day-to-day basis to mitigate the different type of frauds. But the most efficient and important way is the organization's respect to the anti-fraud policy created, ensuring its regular review and updation.

The fraud, if occurred, can cause impact at any level. Hence, the various effective techniques based on emerging technologies like Artificial Intelligence, Machine learning or Data analytics can help us in unearthing the impact of a fraud that occurred. But it's always wise to introduce these technologies to the environment in the form of a defense as well, so that fraud can be prevented to an extent, at the first place.

Continual fraud risk assessment of various business processes also helps to understand the gaps in advance, plan and implement the effective and best suited control to plug in that gap in a timely way.

An organization's culture where all personnel across any level feel confident and safe to report any type of fraud noticed, without the fear of retaliation is a very important aspect to ensure an open environment. This aim can only be achieved when special efforts are being made to ensure the confidentiality of the person reporting the matter till the time it is not important for the investigation of the case.

Summarizing, the organization's culture plays a very critical role in maintaining the fraud free environment. It is pertinent to maintain the healthy organizational culture as it can cause serious impact not only financially, but for bigger companies' reputational loss is even more concerning.

Ranjana Rao

CFE

Head of Security- RIL, Logistics

How investigation and loss mitigation can help insurance business?

The insurance business is built on the foundation of trust, wherein insurers trust that information provided by customers while buying a policy is true and in turn, customers have faith that the insurance company will be there by their side in case of an exigency. Frauds in the insurance industry are rampant which lead to cracks in this foundation of trust. The complex nature of insurance transaction processing, including the extent of reliance on third party service providers, such as assessors, brokers, etc., makes insurers highly susceptible to frauds within and along its value chain. It drives up the cost of insurers, drains their resources thereby leading to increase in prices that a legitimate customer needs to bear. Additionally, it also affects the time taken for claim settlement by the insurers. Here's where investigation and loss mitigation come to their rescue.

Investigation and loss mitigation help defend the business against various fraudulent activities. Deployment of various manual triggers as well as modern and forensic tools can help organizations find the irregularities and enable accurate collection of details, which was earlier difficult using traditional investigation methods. Technology like Artificial Intelligence and Machine Learning and vast amount of data, can help eradicate fraud and minimize the losses. Additionally, deployment of analytics and automated claim scoring mechanisms can increase fraud detection rate, reduce fraud leakage and result in effective evidence collection. This in turn helps insurers to improve their claim processing and fraud detection turnaround time, while reducing customer objections and enhancing their experience.

A preventive fraud scoring model can also be developed at the underwriting level to prevent loss making business at the entry level itself. This can be based on three criteria:

Business experience: Past business experience in terms of sales which have been a risk can help give insights in terms of underwriting new business

Claim experience: Claim trends in a particular city, industry, network partner from where you have received suspicious claims earlier act as a red flag for where not to underwrite new business

Technical tools and Advanced analytics: Tools like that of accident reconstruction, forensics coupled with the power of data can help analyse potential fraudulent activities

India is not far in developing the business rule before underwriting the policy, which can help detect the affinity of claim being negative before the policy is being underwritten. The learning of risk in the claims investigated will help create a risk feed for business rule engine to increase the agility and efficiency.

Adaptation and integration of the data of the entire industry on one platform is going to be the future preventive approach to curb business losses. Work has already started in this direction. The General Insurance Council in India, in collaboration with the entire insurance industry has come up with fraud repository portal and contributory database model, which will help companies identify blacklisted entities and individuals at the time of underwriting policy and claim level.

A better loss prevention framework in insurance companies translates directly into claims cost reduction and portfolio optimization, and indirectly into better services to clients. Smart business means doing your best to do things right the first time.

Sanjiv Dwivedi

Head – Investigation & Loss Mitigation,

Bajaj Allianz General Insurance

Modern organizations can take traditional strides for fraud mitigation!

Today's corporate world is a confluence of organizations that were built decades back and the ones that have been around for much lesser time. There are many differences in the way younger and more modern organizations operate. We all know these differences and the overarching word that is usually used to describe these differences or let us say 'uniqueness' is **culture**!

Yes, its rewarding to change with times and we have seen far more younger organizations growing exponentially in value in much shorter time span. However, being new age does not necessarily mean age-old practices are obsolete. A striking example is "**core values**" – the values we operate on have evolved but the fundamental of operating on core values remains the same.

Let us look at some traditional terms that can help fraud mitigation in modern times –

Loyalty

Most modern-day workforce might chuckle at the word 'loyalty' because they associate it with longer tenures and today many employees move around different organizations with tenures as less as 1-2 years per organization. Modern day organizations must focus on absorbing this term and evolve its definition to nurture a sense of belongingness to the organization without any clause on tenures. This will bolster mutual respect between employees and organizations. Any individual who has a sense of belonging and respect will tend less to sway towards malpractice against the organization and chances of them being a brand ambassador of such organization event after they have moved on is high.

Documentation and accountability

Today's world relies on IT enablement and audit trails for documentation norms. Traditionally, the impetus on documentation was extremely high and there was an inherent accountability associated with every signature.

Modern day organizations must reinforce the documentation practices by constantly reinforcing the accountability every email, meeting, system access, etc. that maps the e-Signatures of the employees via their laptops, cell phones, etc. This reinforced accountability will help create a much robust deterrent against fraudulent practices.

Investing in workforce

In my personal observation, I have noted over the years many organizations, old and new alike have developed policies and changed older practices to optimize cost. A few examples – leave encashment, CTC restructuring, perquisites, allowances, etc. are constantly tweaked. This does create a sense amongst the workforce about in lines with how much organizations values its employees. Modern day organizations must not overlook this aspect or observations and ensure parity in practices that not only benefit the organization alone but also its employees. This helps in maintaining higher engagement levels thereby improving organizational defenses against frauds.

These are just some of the many such practices and values. I am sure all of us can think of many more. It is important to learn from the past as we work hard in our present for a secured and sustainable future. Just as environmentalists talk about leaving a better place for future generations, us professionals must also do our bit to create a better working environment for future generations. Modern organizations are in the forefront of this change and traditional practices can offer important wisdom not just for fraud mitigation, but all aspects in this working world.

Dhaval Mehta

DGM, Business Ethics and Compliance

Lupin Ltd.

Compliance and anti-fraud controls during crisis scenarios: **now, next and beyond!**

For most organizations, the 'Now' phase of their crisis plan has already passed. However, many companies are still operating amid some restrictions. The 'Next' and 'Beyond' phase highlight areas of focus from an anti-fraud and compliance standpoint as corporates move toward recovery and revival.

Now

Crisis Management
(Establishing cross functional COVID 19 taskforce)

People Centric Initiatives
(Revisiting "Work from home" guidelines, sentiments, monitoring behaviour)

Supply Chain Management
(Reviewing third party viability – i.e. liquidity, ownership etc.)

Cyber Incident Response Plan
(Cyber security, Sensitising staff around malware, phishing, ransomware attacks)

Reviewing Contracts, Disputes
(Impact assessment, obligation analysis of contracts)

Next

Conducting Fraud Risk Assessment
(Re-evaluation of Anti-fraud framework)

Revisiting Technology Infrastructure
(Modernizing existing cloud environment, enterprise collaboration)

Relooking Third Party Risks
(Liquidity risk assessment, market reputation as a part of vendor evaluation)

Digital Training Capsules
(Tone at the tone, code of conduct trainings)

Building Resilience
(Holistic models for rapid crisis management, respond to risks etc)

Beyond

Focusing on Ethical Growth
(Creating a culture of integrity and sustainability)

Leveraging Emerging Tech.
(Automation, AI and RPM for process improvements, compliance etc,)

Continuous Monitoring
(Monitoring of Transactions, emails, third party)

Re – examining Legal Agreements
(Benchmarking of legal contracts against best practices)

Prioritizing Compliance in CSR
(Compliance with laws and internal policies in CSR spends)

Quantifying crime or fraud

Every crime or fraud has a cascading effect on the economics associated with it. The Police enter details of property stolen, property recovered, weapons used, suspects arrested, suspects sent for trial with outcome of such trial etc. Corporate investigators, on the other hand, upload records of investigation including statements and investigation report. While this is all good and required, the physical, financial, regulatory and emotional impact any crime or fraud can sometimes be devastating, for those involved and even to the concerned corporate entity.

As far as corporate investigations are concerned, an investigation may lead to loss of business, loss of employment, and risk – reputational, regulatory and financial. Like an iceberg, the loss recorded in the case management system may sometimes be very minuscule as compared to the actual loss that is not apparent or immediately verifiable.

According to an old adage, “A milch cow gets the juiciest fodder while the heifer goes to the slaughterhouse”. This is true for the investigating units in corporates as well. The corporate investigation units are considered as non-revenue generating units of the corporate. Resultantly, these units do not generally get due attention or recognition as compared to the revenue generating units.

With the help of few cases, both from my law enforcement days as well as while working as an investigator in multi-national banks, an attempt is hereby made to explain quantification of crime or fraud and thereby its impact either on the society, the exchequer or the concerned corporate entity.

In the year 2000, the Mumbai Unit of the Anti-Corruption Bureau (ACB) arrested a BMC Vigilance Inspector for demanding and accepting bribe of Rs. 32,000 from a transport contractor for releasing a truck that the Vigilance Inspector had impounded for evasion of octroi. The ACB and Court records rightly captured amount of bribe demanded, amount of bribe accepted and person arrested. However, beyond what is required to be captured in the case management system or the crime register, an effort was made to quantify this crime and its impact.

The Greater Mumbai Municipal Corporation (then) had six octroi collection check posts. The ACB called for statistics relating to the daily collection of octroi for three months prior to the date of the trap and three months post the arrest of the Vigilance Inspector. The results were startling. It was disclosed that daily collection of octroi at the six check posts, till date of arrest of the Vigilance Inspector was approx. Rs. 6 crores. This amount increased to approx. Rs. 12 crores per day after arrest of the Vigilance Inspector. I will leave it to the imagination of the reader to calculate the loss to exchequer per year and its implications to the development of this island city and on the society at large.

During my service with a multi-national bank, it was suspected that a small group of employees had submitted forged or fake food bills while on a short-term international project assignment. The employees concerned, were supposed to submit bills to claim income-tax relief on their per diem entitlement. Investigations disclosed that it was not just the few reported employees who had submitted forged or fake food bills, there were hundreds of such employees who had submitted thousands of forged or fake food bills to claim rebate in income tax. While action was taken against the employees concerned, computing and managing the subsequent tax liability of the employer’s part, including retrospectively, required huge efforts and resources. The employees had saved a few hundred rupees of their tax liability, but the employer bank had to spend millions to rectify the situation.

Corporate frauds like Satyam, Enron, Wells Fargo, WorldCom, Lehman Brothers Bank, Barings Bank usually end up in the concerned corporates either declaring insolvency and/or investors losing billions overnight, not to mention the protracted legal costs and court cases in various courts and countries.

From the above cited examples, it can be seen that any major corporate fraud has huge impact on many stakeholders, including other employees of the company and importantly, the shareholders. The Punjab and Maharashtra Cooperative Bank fraud, as an example, has had a huge impact on the entire cooperative banking sector with customers generally starting to disbelieve the cooperative banking sector.

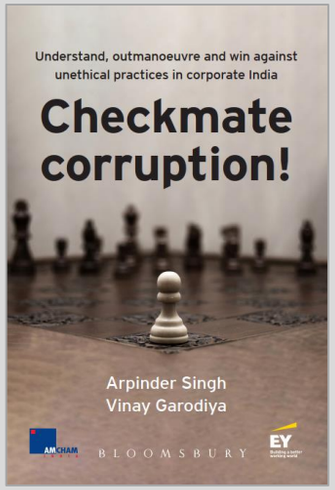
Quantifying fraud, therefore, needs attention as a matter of policy. This cannot be left entirely to the investigators. Quantifying a fraud should be an ongoing process and hence needs constant attention by a group of individuals from various Risk Containment Units. It is important that while quantifying any fraud, every aspect or impact of it needs to be quantified and documented at one place, which can be the case management system of the corporate entity concerned.

Arun Wable

B.Sc. DCC. DCF, CFE, CFAP

Author of the book – The Science of Eliciting Truth, a handbook on Investigative Interviewing and Interrogation for Corporate Investigators.

Grab a copy of **‘Checkmate corruption!’**



The constant battle between corruption and anti-corruption is strikingly similar to a game of chess, with two opposing sides pitted against each other, each fiercely committed to achieving its own goal. Chess is a thinker’s game, requiring extraordinary patience, planning and strategy. Published by Bloomsbury India, ‘Checkmate corruption!’ looks closely at the various dynamics that transpire between corrupt and ethical forces. It highlights the impact of actions, with various chess pieces imbibing certain personas or characteristics, as is found in the corruption and anti-corruption ecosystem.

Some of these pieces may operate at a fundamental level, while others do so at a more strategic one. The book further describes different components, attitudes, activities, rationalization and repercussions in a business environment. In the end, the “checkmate” effect is determined on perpetrators, who will no longer be able to consider themselves safe if unethical practices are followed. The book is authored by Arpinder Singh, Partner and Head, India and Emerging Markets, Forensic & Integrity Services, EY and Vinay Garodiya, Partner, Forensic & Integrity Services, EY.

Amazon: **https://amzn.to/3mcod4y**

MeriPustak: **https://bit.ly/3dNQBad**

MakeMyDelivery: **https://bit.ly/35qlayS**

Five fraud tips every business leader should act on!

Organizations worldwide lose an estimated 5% of their annual revenues to fraud, according to the ACFE's 2016 Report to the Nations on Occupational Fraud and Abuse. A single instance of fraud can be devastating: the median loss per fraud case was $145,000, and more than a fifth of the cases involved losses of at least $1 million.

The good news?

There are some basic steps your organization can take immediately to lessen your vulnerability to fraud.

01 **Be Proactive:** Adopt a code of ethics for management and employees. Evaluate your internal controls for effectiveness and identify areas of the business that are vulnerable to fraud.

02 **Establish Hiring Procedures:** When hiring staff, conduct thorough background investigations. Check educational, credit and employment history (as permitted by law), as well as references.

03 **Train Employees in Fraud Prevention:** Do workers know the warning signs of fraud? Ensure that staff members know basic fraud prevention techniques.

04 **Implement a Whistleblowing Hotline:** Fraud is still most likely to be detected by a tip. Providing an anonymous reporting system for your employees, contractors and clients will help uncover more fraud.

05 **Increase the Perception of Detection:** Communicate regularly to staff about anti-fraud policies, ways to report suspicions of misconduct, and the potential consequences (including termination and prosecution) of fraudulent behaviour.

Source: https://www.fraudweek.com/fraudweek/resources

What is International Fraud Awareness Week?

International Fraud Awareness Week is led by ACFE, the world's largest anti-fraud organization and premier provider of anti-fraud training and education with more than 85,000 members. Fraud Week champions the need to proactively fight fraud and help safeguard business and investments from the growing fraud problem. In 2020, this movement is from 15 to 21 November. During Fraud Week, official supporters will engage in various activities, including: hosting fraud awareness training for employees and/or the community, conducting employee surveys to assess levels of fraud awareness within their organization, posting articles on company websites and in newsletters and teaming up with local media to highlight the problem of fraud.

ACFE Mumbai Chapter and EY Forensics 'Anti-FraudXChange' knowledge sharing virtual sessions

We're hosting a series of webinars during Fraud Week on emerging trends to mitigate fraud, measures taken by various companies, and related topics. In these virtual sessions, industry thought leaders and senior Chapter members will share latest fraud prevention trends and how organizations can proactively prepare for and minimize the risk of fraud and non-compliance.

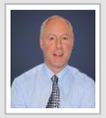
Schedule

18 November

4:30 - 6:30 pm IST

Session 1: Global Compliance Trends

By Basha Galvin, Chief Operating Officer, Association of Corporate Investigators



Steve Young, Chief Executive Officer, Association of Corporate Investigators

Session 2: Cross Border Investigations

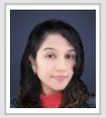
By Percy Amalsadiwalla, Chief Manager - Investigations & Regulatory, Siemens

Link: https://bit.ly/2Uzac5k

19 November

4:00 – 6:00 pm IST

Session 1: Risk Assessment (Compliance Risk reporting & Self-Monitoring tools)



By Deepa Bhandare, Compliance Officer – HC India & Thailand, Merck India

Session 2: Fraud detection and deterrence: an internal auditor's perspective

By Manoj Agarwal, Head - Internal Audit and Risk Management, Metro Brands

Link: https://bit.ly/35DOvY6

20 November

4:00 – 6:00 pm IST

Session 1: Managing third party compliance risks – The Medtronic Compliance Program

By Tanhieya Ghosh, Director- Legal & Compliance, India Subcontinent (India & South Asia), Medtronic

Session 2: Data privacy in a pandemic induced environment: compliance constraint vs control

By Atul Juvle, General Counsel, Compliance Officer & CS- India & SA, Schindler

Link: https://bit.ly/3f8H0eI

Arpinder Singh
President and Founder, ACFE Mumbai Chapter and Partner and Head - India and Emerging Markets, Forensic & Integrity Services, EY

Amit Rahane
Vice President, ACFE Mumbai Chapter and Partner, Forensic & Integrity Services, EY India

International Anti-Corruption Day –
Recover with Integrity

United Nations Office on Drugs and Crime (UNODC) observes Anti-Corruption Day on 9 December every year.
Join EY Forensics at the Association of Corporate Investigator's (ACi) live webinar on 'Fraud, Bribery & Corruption in Asia' on Monday 7 December from 1.30-2.30 pm IST.

Register here: https://www.my-aci.com/fraud-investigations-in-asia.html

About ACFE Mumbai Chapter
The Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with more than 85,000 members, the ACFE is reducing business fraud world-wide and inspiring public confidence in the integrity and objectivity within the profession.

The ACFE Mumbai Chapter #160 was formed in 2011 and is a not-for-profit organization dedicated to fraud prevention education through meetings, seminars, workshops and professional networking opportunities for our members. Usually referred as ACFE Mumbai Chapter, it is registered as “Western Region Chapter of the Association of Certified Fraud Examiners (ACFE), India”.

Follow us on Twitter **@ACFEMumbai**

Join our LinkedIn group **ACFE Mumbai Chapter**

Send your queries to **acfemumbai@gmail.com**

About EY Forensic & Integrity Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

Join the conversation **#EYForensics #FraudWeek #ACFE**

Follow us on **@EY_India**

For help and more information, please contact one of EY Forensic & Integrity Services’ leaders.

Arpinder Singh
Partner and Head – India and Emerging Markets
Direct: + 91 12 4443 0330
Email: arpinder.singh@in.ey.com

Sandeep Baldava
Partner
Direct: + 91 22 6192 0817
Email: sandeep.baldava@in.ey.com

Vivek Aggarwal
Partner
Direct: + 91 12 4443 4551
Email: vivek.aggarwal@in.ey.com

Mukul Shrivastava
Partner
Direct: + 91 22 6192 2777
Email: mukul.shrivastava@in.ey.com

Anurag Kashyap
Partner
Direct: + 91 22 6192 0373
Email: anurag.kashyap@in.ey.com

Rajiv Joshi
Partner
Direct: + 91 22 6192 1569
Email: rajiv.joshi@in.ey.com

Yogen Vaidya
Partner
Direct: + 91 22 6192 2264
Email: yogen.vaidya@in.ey.com

Dinesh Moudgil
Partner
Direct: + 91 22 6192 0584
Email: dinesh.moudgil@in.ey.com

Jagdeep Singh
Partner
Direct: + 91 80 6727 5300
Email: jagdeep.singh@in.ey.com

Amit Rahane
Partner
Direct: + 91 22 6192 3774
Email: amit.rahane@in.ey.com

Vikram Babbar
Partner
Direct: + 91 22 6192 2155
Email: vikram.babbar@in.ey.com

Harshavardhan Godugula
Partner
Direct: + 91 40 6736 2234
Email: harshavardhan.g@in.ey.com

Vinay Garodiya
Partner
Direct: + 91 22 6192 2164
Email: vinay.garodiya@in.ey.com

Saguna Sodhi
Partner
Direct: + 91 12 4443 4353
Email: saguna.sodhi@in.ey.com

Avantika Ghildyal
Vice President – Marketing & Communications
Direct: + 91 22 6192 1026
Email: avantika.ghildyal@in.ey.com