Nangia Andersen LLP

Suspecting a **fraud** in your **organization**?

www.nangia-andersen.com

A member firm of ANDERSENGLOBAL

Here is a quick reference guide of Dos and Don’ts

Covid-19 pandemic has given rise to a widespread disruption in business operations, globally. Consequently, it has exposed the businesses to vulnerabilities of fraud. Spurt of the virus has ushered in a new era of hybrid model of working from home and partially work from office. Such an environment makes corporates more vulnerable to fraudulent practices.

Why read this article?

As per ACFE report “Global study on Occupational fraud and abuse”, many victims had not reported fraud cases to law enforcement agency though the organization had enough reasons to believe that fraud had occurred and, in many cases, even knew the modus operandi and culprits. Respondents, who did not report the case, were asked the reasons for the same. 10%[1] of the victim organizations stated “lack of evidence” to be the key reason. This makes it imperative to understand the significance of evidence collection and preservation. Additionally, the report also indicates that the duration of fraud is directly proportionate to the financial loss on account of the fraud. Hence, taking prompt actions can aid in quick detection of fraud consequently arresting or avoiding the potential loss. This article discusses about such immediate steps recommended to be undertaken on observing any red flags, receiving any whistle blower complaint, or even suspecting a fraud or malpractice. Management may choose to do all or some of the below recommended good practices depending upon the suspicion, seriousness/complexity of fraud, quantum of damage, number of suspected employees, duration of fraud etc.

[1]https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

Need of an Incident Response Plan

Success of an investigation depends on the immediate steps taken by an organization promptly on being acquainted about suspected fraud. Having a comprehensive incident response plan to deal with any fraud situation is the need of every organization irrespective of sector, size or geography. An incident response plan will communicate an organization's responsibilities with respect to preserving evidence along with its safekeeping, securing the workplace of suspect, withdrawal of approving rights, change of login credentials for financial transactions, informing the external vendors.

For each case, management should cautiously identify which individuals should be informed of the required steps of the incident response plan. Similarly, it is important to identify individuals from whom the procedures should be kept completely confidential to avoid tipping off the suspect. For instance, IT head is required to be informed about the suspicion to aid in data extraction while preserving data sanctity, legal head needs to be mindful of handling various legal issues which may arise during & post incident response. However, other individuals working in the ecosystem of suspect employee can be provided with the information on need-to-know basis. Once suspect is aware that eyebrows are being raised on his/her activities, he/she can misguide the potential probe in many ways or devise novel models to destruct the evidence too

Incident response steps:

1. Evidence gathering:

Collection of relevant evidence is critical in proving or disproving the occurrence of fraud. Evidence recreates the sequence of events which uncovers the overall modus operandi used to execute the fraud and also involvement of other individuals or third parties who may not be otherwise in the lens of suspicion. Careful evidence handling becomes significant at the organization level to underpin potential probe and investigation. Evidence resides in two forms, digital and physical, both of which, are equally important for successful completion of investigation

- **Digital evidence**

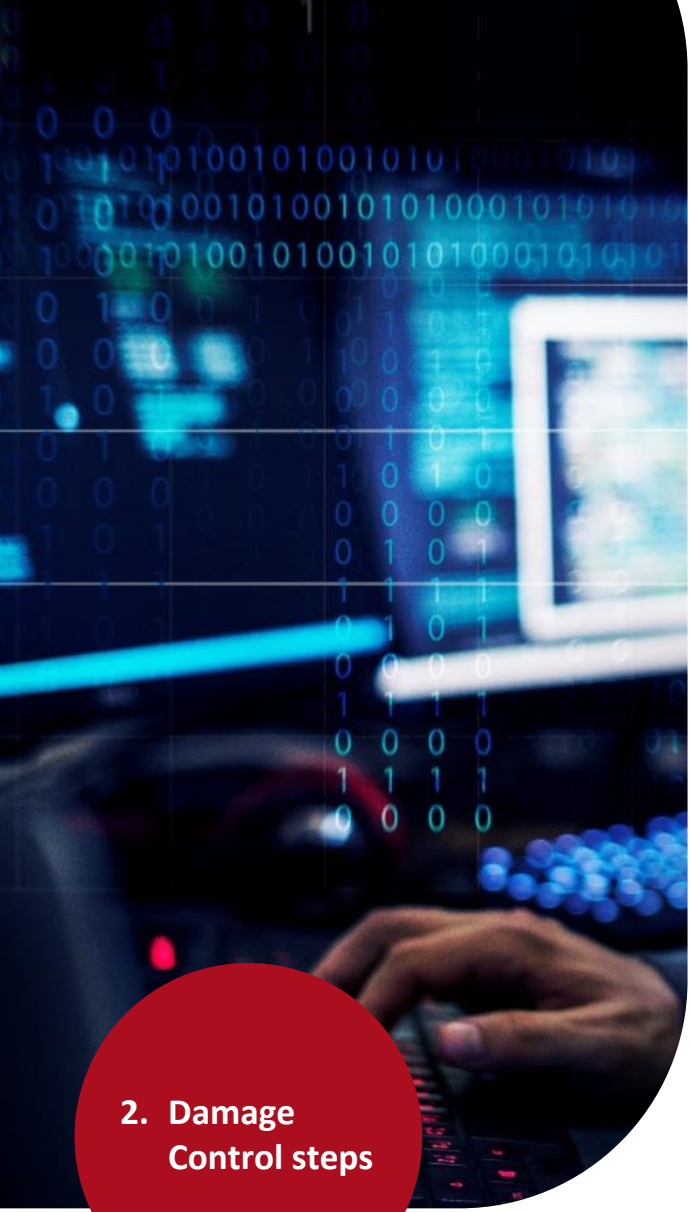
  Enormous data stored in an organizational database is in digital media, which can assist in connecting the dots for a suspected fraud. Digital evidence is available in two data types viz volatile data and non-volatile data.

  Volatile data resides in random access memory (RAM), registries and cache. It includes the information which is currently being run by the computer. Once the computer is turned off, such data is lost. Collecting such data from the suspect's workstation should be undertaken on a priority basis before any power cuts or before switching off the computer. The process of gathering volatile data is also known as "live forensics". However, organization should assess the relevance and applicability of such data with the suspected fraud case.

  Non-volatile data is a part of permanent memory in the computer. Common files containing evidence stored in computer systems include user created files and computer created files.

  - **User created files:** User created files are digital files created under the direction of user. These files include word file, spreadsheet, power point presentation, text-based documents, databases, emails, audio/video files and image files. Such files shall be seized from the suspects computers to scrutinize in search of incriminating evidence.
  - **Computer generated files:** Information generated by a computer's operating system can also be a source to trace the activities of suspect. Some common examples of computer generated data are metadata, event logs, internet activity & deleted data which is explained below:

	Computer generated files	What data does it record?	How can such data help the organization?
1	Meta data	It provides data about who copied, received, clicked, edited, moved, or printed the document; and when these events occurred	It would help gather information regarding the personnel involved in alteration or destruction of evidence
2	Event logs	Event logs records the data about transactions and events taken place on a computer chronologically	A detailed review of event logs can help to understand the timelines of fraudulent activities.
3	Internet activity	It stores the data regarding the websites visited, time spent online & images previously viewed online.	A quick scan over suspect's search history is likely to give clues regarding suspect's behavioural pattern
4	Deleted data	Data are not erased from computer's hard drive until the data are overwritten. Deleted files might be recoverable	Such deleted files might include critical evidence supporting the case



2. Damage Control steps

It is important to handle the data collected with precision and care. Evidence collected must be backed up to avoid damage and alteration of any kind. Relevant information from the suspect's computer is essential to be extracted without alerting the suspect.

- **Physical evidence**

  Before securing the workplace, the first step is to examine and document the target's workplace surrounding. The executive, seizing the workplace, should collect all the documents irrespective of it been relevant or not at the time of seizing. Discarded documents, which are often considered as irrelevant, provide important leads on the suspicion, and hence same should also be preserved with due care. Documents may provide many leads on the information about the suspect's daily activities, passwords, more targets who might be working hand in gloves with the suspect, plans for suspect's future course of actions, etc. The documents handled by the suspect shall be preserved such that it is retained in its original form. Evidence collected must be kept in safe place under lock & key to prevent it from any unauthorized access.

- **Withdrawal of approving rights:**

  Suspect may be the person approving workplans or taking decisions at various level of business operations. It is recommended to suspend the approving rights for various business process and operations in the ERP software to prevent the organization from suffering the consequences resulted from biased decision undertaken under suspect's leadership. No decision under the suspect's KRA should be allowed to take in silo rather be approved/consulted with the senior person.

- **Curb the email outflow:**

  It is recommended to restrict the external mails from the suspect's email ID. This will prevent the suspect to illegally take biased decisions with the external vendors and cause further damage. All incoming emails should be diverted to alternative email to ensure that appropriate and timely response is provided to business related emails from customers/vendors. This activity may be required to be continued even after the suspect has discontinued from the organization.

- **Safeguard the confidential information**

  After restricting the flow of external mails and withdrawal of approving rights, it is recommended to immediately change the passwords of important login credentials specifically which enable the banking/financial transactions to safeguard the misuse of funds by the suspect.

- **Alert your external business associates:**

  Next step should be to approach the external business associates (vendors, customers, dealers, distributors, consultants, regulators, etc.) with whom the suspect undertake dealings on behalf of the organization. The purpose of such a meet with external business associates is to acquaint them about the new single point of contact (SPOC) for the organization and if need be, even disclose the fraud and investigation findings. This would ensure that important information or business deals will not flow to the suspect consequently safeguarding the organization from biased decisions.

3. Identify potential witnesses:

As per ACFE report "Global study on Occupational fraud and abuse", 43%[2] of schemes were detected by tip and half of those tips came from employees. Accordingly, if fraud suspicion had arisen on filing of whistle blower complaint, then organization should immediately encourage the whistle blower to discreetly disclose the information to understand the details of the fraud scheme or provide more details/proof of the fraud. This will not only uncover the modus operandi of the fraud but also assist the organization in timely action to secure evidences. Historically, it is observed that the quicker and more sensitively the discussion/correspondence with the whistle blower are managed, better are chances of successfully closing an investigation.

[2]Ibid

4. Potential suspects:

As per above mentioned ACFE report, 51%[3] of fraud in their study were committed by two or more perpetrators working in collusion. Accordingly, there can be a possibility of more than one suspect executing the fraud scheme. Therefore, the organization should identify such other suspects who might be working hand in gloves with the prime suspect to execute the fraud schemes. Organization should undertake all the incident response steps as mentioned above for such other suspects as well to curb fraud losses.

These are some prerequisite steps which should form part of the incident response plan.

Based on the quantum of fraud and requirement of an organization, an external investigation agency can be appointed to explore the need of detailed investigation. The scope of work of such investigation should include desktop & email review, forensic data analytics, market intelligence, interview with whistle blower (if any) and document review to join different pieces of information and analyse the fraud scheme.

Such an investigation report would assist the organization to identify the loopholes. This can be overcome by implementing strong internal control mechanism commensurate with the organization. In this way, timely action to combat fraud would help the organization to arrest the fraud losses.

[3]Ibid

A Quick checklist on arise of suspicion

- Reporting to competent authority
- Preserving the evidence (both digital and/or otherwise)
- Withdrawal of approving rights
- Restrict the email flow
- Safeguard the confidential information
- Alert your business associates
- Identify potential witnesses and suspects
- Complete the investigation process to confirm or reject the allegations
- File closure report

Meet our Experts

Srinivasa Rao
Partner & Leader - Risk Advisory Services
srinivasa.rao@nangia-andersen.com
+91 96001 13339

Kaushal Mehta
Partner - Forensic Services
kaushal.mehta@nangia-andersen.com
+ 91 98337 37797

Shrikrishna Dikshit
Partner - Cyber Security
shrikrishna.dikshit@nangia-andersen.com
+91 98203 65305

Shravan Prabhu
Partner - Cyber Security
shravan.prabhu@nangia-andersen.com
+91 98190 24009

Tauwfiq Wahidi
Director - Risk Advisory Services
tauwfiq.wahidi@nangia-andersen.com
+91 9967026038

NOIDA
(Delhi NCR - Corporate Office) A-109, Sector - 136, Noida - 201304, India | T: +91 120 5123000

DELHI
(Registered Office) B-27, Soami Nagar, New Delhi – 110017, India | T: +91 0120 5123000

GURUGRAM
812-814, Tower B, Emaar Digital Greens, Sector-61, Gurugram, Haryana - 122102, India
T: +91 0124 430 1551

MUMBAI
11th Floor, B Wing, Peninsula Business Park, Ganpatrao Kadam Marg, Lower Parel, Mumbai - 400013, India
T: +91 22 61737000

CHENNAI
Prestige Palladium Bayan,
Level 5, 129-140, Greams Road, Thousand Lights, Chennai – 600006, India | T: +91 44 46549201

BENGALURU
Prestige Obelisk, Level 4, No 3 Kasturba Road Bengaluru - 560 001, Karnataka, India

PUNE
3rd Floor, Park Plaza, CTS 1085, Ganeshkhind Road, Next to Pune Central Mall, Shivajinagar, Pune – 411005, India

DEHRADUN
1st Floor, "IDA" 46 E.C. Road, Dehradun - 248001, Uttarakhand, India | T: +91 135 271 6300

www.nangia-andersen.com | query@nangia-andersen.com

Follow us at :