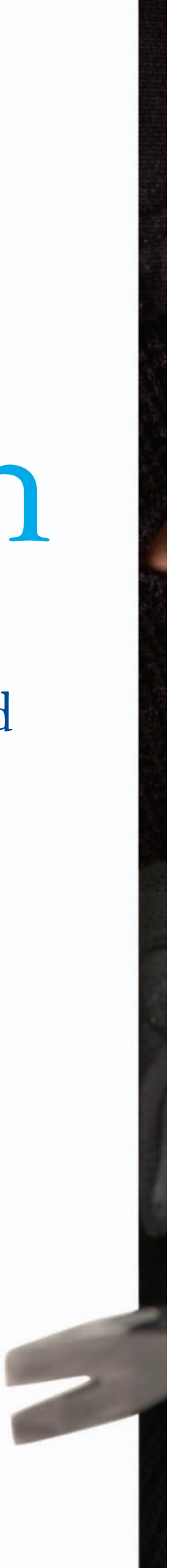
Keep calm

You think you have discovered a fraud. What do you do?

Despite recent surveys pointing to fraud being on the increase, the discovery of a suspected fraud within any organization is not an everyday occurrence for most people and initial reactions may include shock and surprise. However, action taken in the first few hours and days after discovery will significantly impact the course and/or outcome of a full investigation and may even make it or break it.



and carry on.

Most organizations have controls in place to prevent and detect fraud being committed against them from the outside. In the banking industry in particular, external fraud is an expected occurrence and banks employ sophisticated processes and technology to prevent and detect such occurrences. The bigger problem occurs when fraud has been committed from within. Apart from the cost involved, there is always some collateral damage caused including loss of reputation, brand damage and reduced employee morale. Seniority of the suspect is also a factor, the more senior the employee, the more serious the damage.

History shows that, in the absence of any structured response plan, the amount of time and effort it takes for management to respond, particularly in the initial weeks, is excessive and severely impacts the normal business activity of the organization. When a potential fraud is first discovered, the following few hours or days can be very confusing and stressful if the organization is unprepared. In the absence of a Fraud Response Plan, experience has shown that managers handle the same problem in different ways - sometimes with disastrous consequences such as destroying the evidentiary value of information by inappropriate handling processes, inadvertently tipping off the suspect, enabling them to destroy incriminating evidence, failing to keep the matter confidential and taking inappropriate action caused by having insufficient information.

When a potential fraud is first discovered, the following few hours or days can be very confusing and stressful if the organization is unprepared

For example, in a recent fraud incident occurring in the UAE, an employee who was in charge of procurement for a certain organization also operated a supply and contracting company which had been paid in excess of Dhs 3,000,000 by his employer's company, all ordered and authorised by him. The suspect, once discovered, was dismissed but was given a month's grace period during which time he destroyed a large number of incriminating documents.

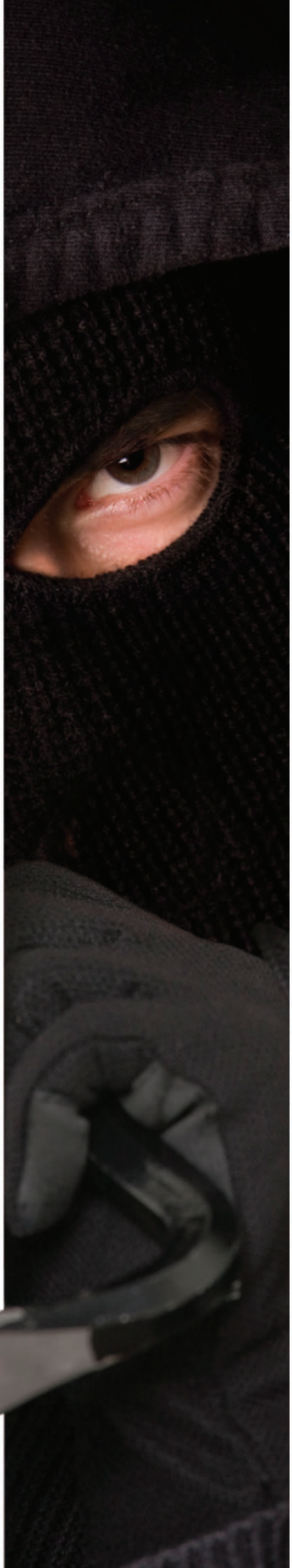
In another incident, it became widely known throughout an organization that a fraud had been uncovered. However, that particular incident, which became public knowledge, was only a small part of a much larger conspiracy between a number of employees and suppliers. By failing to keep the

Fraudsters rarely restrict their activities to only one modus operandi or method. Therefore, every effort should be made to obtain as much information as possible before anyone is questioned, confronted or interviewed.

matter confidential, the company management enabled the conspirators to destroy incriminating records, electronic data and to dispose of stolen property, which rendered any future investigation futile. The identities of the suspects were not confirmed, meaning that the company may still be employing people who are actively seeking ways to defraud it.

A Fraud Response Plan ensures that incidents are handled in a systematic and efficient manner, not only to conclude a successful investigation, but also to show that the organization acted in a prudent and lawful manner. And that it does not tolerate fraud.

The Fraud Response Plan should outline how far an individual line manager should go in collecting initial information before invoking the Response Plan. The key is to provide the line manager with an effective framework to resolve concerns, rather than leave such resolution to individual initiative.



Initial Action

It is important to remember that when fraud is first suspected, the matter may well be more serious than it may initially appear. This is because fraudsters rarely restrict their activities to only one modus operandi or method. Therefore, every effort should be made to obtain as much information as possible before anyone is questioned, confronted or interviewed. This is particularly important in organizations or business units with a close working environment, where there may be a strong temptation to simply question an employee as soon as suspicion is raised.

It is also important to be aware that larger scale frauds are often international in nature. Therefore, any fraud contingency planning must include measures for taking legal and investigative action across jurisdictions.

In addition, most frauds involve the use of a computer at some stage in the planning or execution of the fraud. This is particularly evident in today's environment, when the majority of white collar employees are allocated a computer by their employer. Business is conducted by computer and correspondence normally involves a computer through the widespread use of corporate e-mail. The pervasive involvement of the computer into most facets of corporate life means that electronic evidence is often vital to investigating corporate fraud. Obtaining that electronic piece of evidence is a specialist skill which should be discussed with your forensic specialists.

Initial actions are crucial to the eventual outcome of an investigation and, if a proper strategy is put in place and adhered to, the extent of fraudulent activity can usually be assessed and action taken to resolve the matter successfully. This usually means assimilating sufficient evidence to dismiss errant staff and to commence civil and/or criminal proceedings against those concerned in the fraud, or claims against insurers, if so desired.

It is vital that all allegations of fraud are treated seriously and that responsibility for handling fraud incidents is assigned to a senior, trusted individual or collection of individuals

Initial responsibility designation

Fraud investigation is, by necessity, a confidential task and is a sensitive matter for the vast majority of organizations. It is vital that all allegations of fraud are treated seriously and that responsibility for handling fraud incidents is assigned to a senior, trusted individual or collection of individuals. In many organizations, that responsibility is handed to a corporate security advisor, internal audit manager or risk management director. In other organizations, the responsibility is shared between members of senior management or an audit committee and the organization's human resources personnel and corporate lawyers are involved from a very early point. Fraud incident management responsibility is an important role and those chosen to administer the role must come from the appropriate legal and management level to authorise investigative actions and to co-ordinate the organization's overall response to fraud incidents.

As part of their overall fraud control plan, organizations should assign responsibility for fraud incident management to an appropriate person(s) as a precursor to adopting an incident management plan. Consideration should also be given to the appropriate level of involvement by corporate lawyers and human resource personnel.

Most frauds involve the use of a computer at some stage in the planning or execution of the fraud. This is particularly evident in today's environment, when the majority of white collar employees are allocated a computer by their employer.

Fraud Response Team

Some Fraud Response Plans only deal with situations where an employee discovers a fraud and hands it over to an investigation department to follow up. However, some frauds have impacts far beyond the remit of the investigation department to deal with (such as when the organization's liquidity is threatened). The Plan also should cater for these eventualities.

Most large organizations have formed crisis management committees to respond to major incidents (such as a fire or explosion), so it is not uncommon to take a similar approach in a Fraud Response Plan. Typically, this means forming a Fraud Incident Management Team, comprising essential members and co-opted members.

In some types of fraud, the victim may only have a few hours to take action to freeze funds which have been illicitly transferred. It is essential that contact numbers for essential service providers are established beforehand, including internal support departments, such as legal, corporate security, insurance external lawyers, police and telecommunications agencies, forensic accountants and investigators.

Receipt and initial assessment of suspicion, allegation or 'tip off'

Fraud investigations are often initiated after an allegation or a tip-off (often anonymous) is received. This will usually be sourced from inside the organization, although external tip-offs are not uncommon. Many fraud incidents are initially discovered by accident, perhaps as a result of an audit, job change or resignation. Very few frauds are discovered as part of a deliberate attempt to uncover fraud, as very few organizations implement a proactive fraud detection program.

The checklist on the right/left highlights initial actions to be taken (or not) upon the discovery of fraud or tip-off.

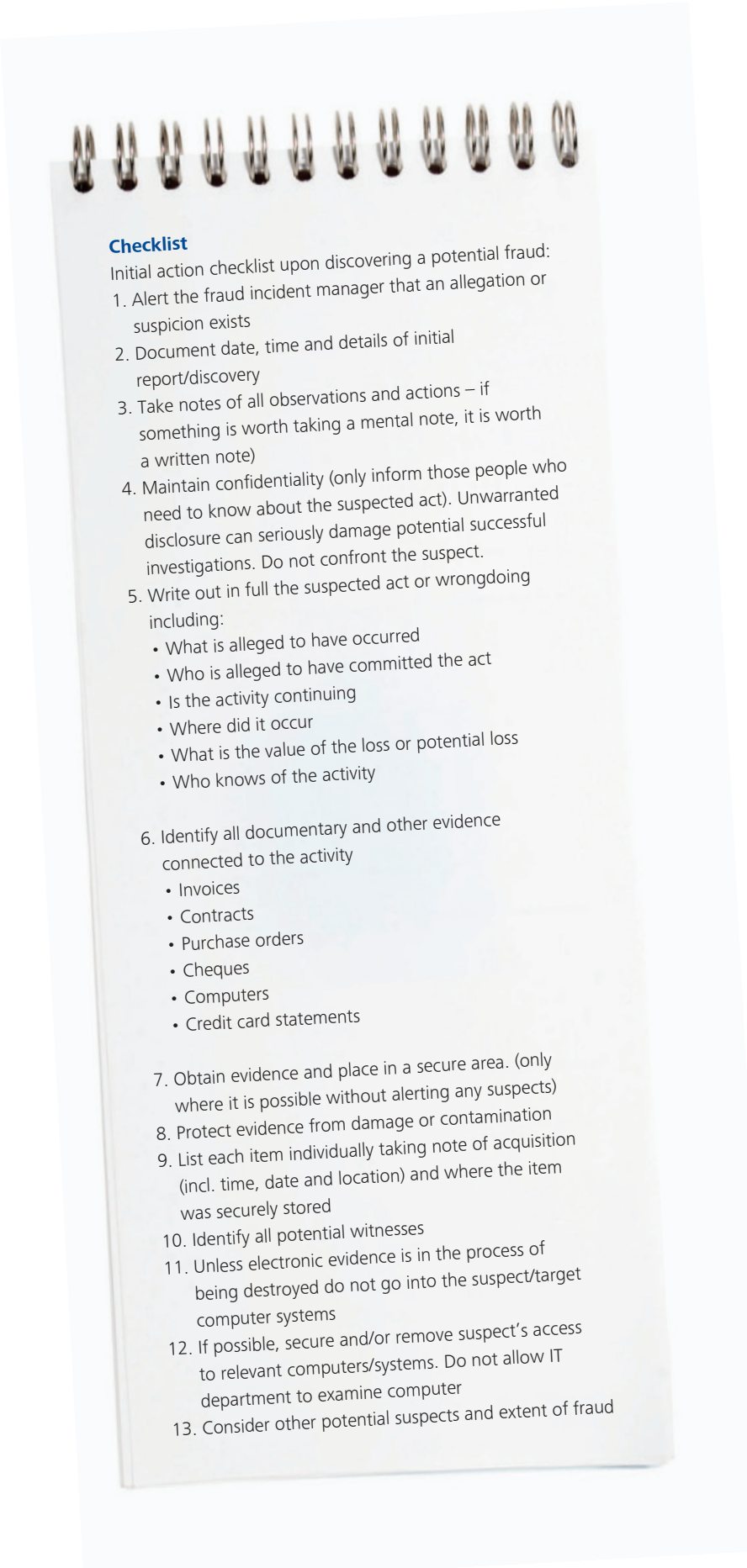
At the conclusion of this stage, a decision must be made as to whether the allegation or suspicion warrants investigation or is implausible or vexatious. However, this decision must be made carefully. If an allegation cannot be quickly dismissed as false, further action should be taken.

A typical Fraud Response Plan contains:

- purpose of the plan,
- policy statement,
- definition of fraud,
- roles and responsibilities including fraud response team,
- objectives including civil and criminal response,
- reporting of suspicions and collection and preservation of evidence.

As part of their overall fraud control plan, organizations should assign responsibility for fraud incident management to an appropriate person(s) as a precursor to adopting an incident management plan

by **David Clements**, director, Forensic and Dispute Services, Deloitte Corporate Finance Ltd



Checklist

Initial action checklist upon discovering a potential fraud:

1. Alert the fraud incident manager that an allegation or suspicion exists
2. Document date, time and details of initial report/discovery
3. Take notes of all observations and actions – if something is worth taking a mental note, it is worth a written note)
4. Maintain confidentiality (only inform those people who need to know about the suspected act). Unwarranted disclosure can seriously damage potential successful investigations. Do not confront the suspect.
5. Write out in full the suspected act or wrongdoing including:
   - What is alleged to have occurred
   - Who is alleged to have committed the act
   - Is the activity continuing
   - Where did it occur
   - What is the value of the loss or potential loss
   - Who knows of the activity
6. Identify all documentary and other evidence connected to the activity
   - Invoices
   - Contracts
   - Purchase orders
   - Cheques
   - Computers
   - Credit card statements
7. Obtain evidence and place in a secure area. (only where it is possible without alerting any suspects)
8. Protect evidence from damage or contamination
9. List each item individually taking note of acquisition (incl. time, date and location) and where the item was securely stored
10. Identify all potential witnesses
11. Unless electronic evidence is in the process of being destroyed do not go into the suspect/target computer systems
12. If possible, secure and/or remove suspect's access to relevant computers/systems. Do not allow IT department to examine computer
13. Consider other potential suspects and extent of fraud