FRAUD AND THE INTERNAL AUDITOR: 
WHAT TO DO AND WHEN YOU FIND IT

In many cases, internal fraud and theft go on for years and are then discovered through internal audit reviews. This is despite numerous red flags being overlooked by co-workers and management. Once identified, internal auditors who lack experience in the area of fraud, may well mishandle the evidence and put a successful prosecution at risk. This presentation will look at the red flags, what the internal auditor should do, how management reacts, and ways to reduce the risk of fraud and/or theft. These will be reinforced by reviewing a number of cases and discussing where the red flags were overlooked or ignored.

COLIN PARCHER, CFE
Private Consultant
United Kingdom

Colin Parcher spent over 30 years in law enforcement and regulatory compliance in Canada. During his career, he has led numerous high-profile investigations, as well as leading a team of investigators whose primary role was investigating fraud and ensuring regulatory compliance within the financial services sector. Being a British citizen, he relocated to the United Kingdom in 2010 where, through his own consulting business, he investigates bribery and corruption as well as providing fraud prevention, detection, and investigation services to private industry. Colin served as a director of the Vancouver Canada ACFE Chapter for seven years and as president for four years. Colin has presented at the ACFE’s National Conference, the Canadian Conference, numerous chapter hosted events, as well as at a wide variety of training events on fraud related subjects to law enforcement and private industry.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
There Is Fraud and Theft Occurring in the Workplace?

Simple Answer: Yes

This likely no surprise to anyone here, as many of us have seen it occur, investigated it, or been victims of it plus report after report has told us just that. It is a major problem and the primary suspects are the employees not outsiders.

A simple Google search of Work Place Fraud gets 98 million hits in 0.37 seconds likewise a Google search of Employee Theft nets 26 million hits in 0.19 seconds—good on Google for being so fast but reality is we do have a problem that is growing fast.

The Canadian Broadcasting Corporation in Canada, which has about ½ as many people as the England, reported in December 2011 that employee fraud was costing small business $3.5 billion (CAN) a year which equates to approximately £2.3 billion.

One UK report says senior managers are now committing more fraud in the work place and another puts the cost to UK businesses in the area of; Padding’ expenses and overtime, theft of office stationery, and even the popping of personal mail into company post, at approximately £15 billion annually.

Who Is the Perpetrator?

It is well known employees will steal from their employers; in fact approximately 80% of employees will commit fraud or theft in their work place. Of that 80% there are 20% you will never stop, they will do it no matter what and this will range in scope, complexity and method. The good thing is there are 20% who won’t steal a thing—if they take a pen home tonight, it comes back tomorrow. They actually buy paper for their home printers and batteries for their children’s electronic birthday gifts.
This brings to the remaining 60%—these are employees who we can call “Swingers”, they might or they might not—it depends on many things: the mood of the moment, the culture of the organisation, the tone at the top, how great the opportunity and how they are compensated to name just a few.

Is this changing, well if you believe a 2009 news report, four out of five UK employees think is okay to steal from their employer. So it may be changing but not in the right direction.

The thieving employees do not have a set profile, it could be a long time (believed to be) loyal or a new hire. However; studies have shown that long term employees are more likely to steal from you. As well they could be of either sex or span a wide range in age

**Charge Them and We Set Examples?**
The Fraud Act 2006 replaced the eight deception offences of Theft Act of 1968 and 1978 with two offences, Fraud and Dishonestly Obtaining Services, plus if you throw in the simple offence of Theft you have three easy charges for the police to use against those who steal from or defraud their employer.

So why are not bring people who are costing employers across the country and around the world before the courts to set an example, surely a few in jail sentences will deter some of this behaviour.

Reality is there are a number of factors coming into play, it will be difficult for you to get an already over worked police force interested in someone stealing two packs of A4 paper. Even if you get the report taken the question will be—will charges will ever get processed. Naturally as the
scope or profile of the offence increases, the chance of a law enforcement agency getting interested.

But even if you want charges and grow frustrated with the system do not take matters into your own hands as one Essex business man did. He got charged and ended up paying the thief £11,000 plus £2,000 in legal costs.

The other factor at play is the employers themselves, they don’t want to pursue charges for reasons of un-wanted publicity, costs and the knowledge that end penalty is not adequate considering the effort to go the legal route.

As a result the more often used route is to try and recover what is recoverable and terminate the employee. Unfortunately these employees often have a sense of entitlement and want to take action for wrongful dismissal, again leaving employers in the position of paying out or getting the dreaded publicity.

The Questions: How Do They Do It?
Why Do They Do It?
Employee fraud and/or theft can take place in a wide variety of ways, to name just a few it could be:

- Compromising the books, customer or payroll data;
- Straight-forward theft;
- The submission of inflated expenses;
- A completely unplanned attacks - An opportunistic moment;
- Purely for personal financial gain; or,
- Part of an organized group.

The list of methods for stealing and defrauding your employer is endless. It is only restricted by lack of imagination of the crooks themselves and their fear that they might get caught.
The crooked employee will have justification for their action but it is often ruled by the GONE-R Theory.

This is Greed, Opportunity, Need, Expectation, and backed up by Rationalization.

While a vast majority of society have a bit of greediness in their personality, many never display especially if the opportunity does not present itself. However if the opportunity presents itself our 60% in the middle may be swayed. Need, on the other hand is a self-determination issue, what one person thinks they need and what someone else thinks they need are often miles apart, so when an individual decides they are going to take something from the employer they will justify it with the “I need that” thought. Expectations of employees are often created by situation with in the work place, where an employee feels they have not been compensated adequately or they perceive another employee is being favoured. This results in their conduct to create a level playing field as they steal or defraud the employer to get what they think they deserve.

Anyone of these will be present in most employees however when you put them all together you have an employee who will steal from their employer.

Once they go down this path they will find ways to rationalize their behaviour as being acceptable with things like the boss takes paper home or everyone else does it.

**Indicators of an Employee Gone Bad**

There are many indicators which may indicate an employee is up to something that is benefiting them, not their employer. Often these indicators are over looked for months or even years. A few of these are:
### FRAUD AND THE INTERNAL AUDITOR: WHAT TO DO WHEN YOU FIND IT

- Staff under stress without a high workload
- Marked personality changes
- Always working late
- Reluctance to take vacation/holidays
- Unexplained wealth or living beyond apparent means
- Customer complaints of missing statements, unrecognized transactions
- Cozy relationships with suppliers/contractors
- Suppliers/contractors who insist on dealing with just one individual
- Rising costs with no explanation
- Key employees having too much control or authority without audit checks
- Employees with external business interests

There are numerous other red flags but the real one that is often overlooked is the over worked employee who works late and does not take vacation—they are often viewed as the “best” when in fact they are the “worst”. The key is for management to be alert for any indicator.

#### How Do We Identify a Problem?

Internal fraud is identified through several basic methods; the employee has an accident or is not able to work for medical reasons, a whistle blower or tip line, through regular and irregular audits or by accident. Based on ACFE figures 34% of internal fraud is identified through tipsters and 25% by accident.

While this does not look good for auditors, the fact is that few companies put resources into irregular or random audits and the regular audit process is not designed to identify fraud. Unless there has already been a problem identified and forensic staff are brought in, may frauds will be missed.
The Auditors Think They Have Found A Problem: Now What?
This is where things start to go wrong, as auditors are exactly that auditors, for the most part they are not trained to deal with matters which going to end in civil or criminal litigation. They are they to check the books and records ensure everything appears to be done properly and the company is in compliance with their regulator. Unfortunately these checks do not identify fraud that has been ongoing for months and years.

All too often you will see the auditor with pencil in had making notes, check marks or writings on documents, or with the yellow marker highlighting information to assist them at a later point in the audit.

The when something does not look right they question it, as they should, but at first they will not believe what they see, so they do what they do very well, they dig deeper, making their notes going through the documents so they can validate what they believe has occurred. Once they happy with their findings that a there is something amiss they report it so an investigation can be commenced.

What Went Wrong Here?
What often goes wrong in these cases is very simple—every document written on, highlighted and handled is now contaminated. This does not say it is inadmissible, but rather the process of getting that document in as evidence could be more difficult.

Once an auditor has the slightest suspicion of a fraud they would be well advised to very carefully handle any documents (only by corners) noting where they touched it, make a copy and then place the document in a protective evidence envelope or sleeve. The protective sleeve should
be marked for identification purposes prior to placing the
document inside so that unexplainable pen impressions are
not made on the document. From that point on, until there
suspicion has been confirmed, or proven to be wrong, every
document must be treated as evidence and handled
accordingly.

This is also the case with computerized audits, at the
slightest indication that something is amiss, the computer
should be secured, an image made by a trained expert, and
all further examination is done off the image while the
original hard drive is properly secured as evidence.

If you believe there is a problem and you do not have an
expert available:

- Avoid touching exposed wiring or circuits.
- If it is Off—Leave it Off
- If it is on—note any running applications; photograph
  the screen & note the date & time.
- If running, unplug it then label the wires and the ports
  they were removed from
- Note serial #s and models of all hardware
- Seize all the components of the system.
- Never turn it on to “Just Check”—you will delete or
  change files.
- Seize all notepads, sticky notes, floppy disks around the
  computer—Small devices store a lot.
- Store extra hard drives in anti-static bags or
  paper/cardboard—do not bump or drop.

An additional problem arises when the work day ends and
the auditors head for home. In many cases they are working
from an office or room where they can spread out but still
be assessable to the appropriate staff to ask questions and
retrieve additional material. At the end of the day they lock
the door and are gone, but who has keys?
What about the room, after all the fraudster has been watching all day and wondering if they will be caught. They will be especially aware of sudden gatherings by the auditors and special attention spent in one area. Once the auditors are gone they will be free to do a bit examination of their own, after all this is the “best” employee who often works late and never takes time off.

So we look at what goes wrong:
- Failure to believe what they see
- Failure to record details properly at the start
- Failure to secure the evidence promptly
- Assuming evidence is secured by moving it to a locked room
- Not applying criminal inquiry standards
- Overlooking computer-based evidence
- Over-enthusiastic examination of computer evidence
- Not using an expert
- Tunnel vision

In every case it is better to error on the side of caution rather than try and fix it later.

**Prevention: What the Employer Can Do**

Some basic steps for the employer to deter (you will never stop it) internal theft and fraud are:
- Create a positive work environment—work on the 60%
- Implement internal controls
  - Separation of duties
  - Access controls
  - Authorization controls
- Hire honest people—regular background checks
- Pay attention—who are their friends
- Implement an anonymous reporting system—take it serious and reward
- Perform regular audits—and irregular audits
<table>
<thead>
<tr>
<th>FRAUD AND THE INTERNAL AUDITOR: WHAT TO DO WHEN YOU FIND IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Investigate every incident—create a culture</td>
</tr>
<tr>
<td>❑ Lead by example—what the boss does so will they</td>
</tr>
<tr>
<td>❑ Know who has bank account access.</td>
</tr>
<tr>
<td>❑ Secure and monitor supplies.</td>
</tr>
<tr>
<td>❑ Make your policies public.</td>
</tr>
<tr>
<td>❑ Treat employees with respect.</td>
</tr>
<tr>
<td>❑ Create a positive culture.</td>
</tr>
<tr>
<td>And remember:</td>
</tr>
<tr>
<td><strong>One Key Point: Focus on Prevention not Detection</strong></td>
</tr>
</tbody>
</table>