Nigel Iyer

How to Find Fraud and Corruption

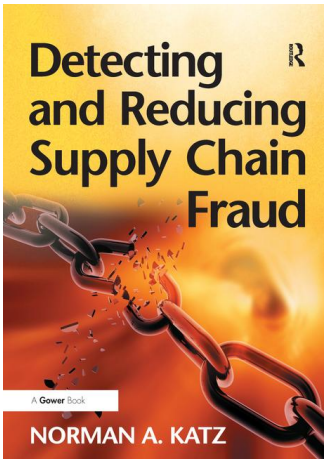
Recipes for the Aspiring Fraud Detective

Special extract of Chapter 5 'Thinking Like A Thief'

Prepared for participants to the "Insights of a Fraud Detective" webinar hosted by the ICAEW- 3rd July 2020 (courtesy of T&F)

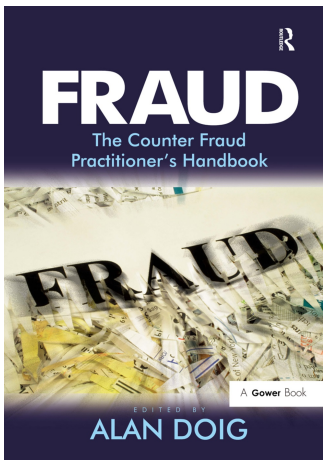
GET 20% OFF WITH DISCOUNT CODE **SOC20**

Other fraud titles you may find useful...



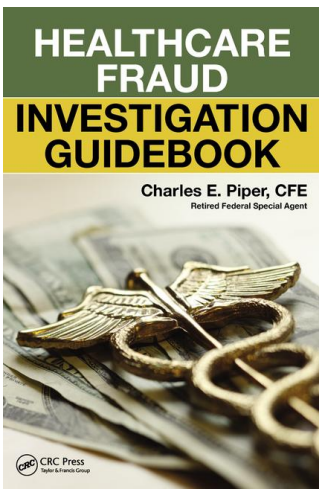
Detecting and Reducing Supply Chain Fraud is a pragmatic guide to identifying and managing sources of risk. Norman A. Katz explains the main categories of fraud risk: what they are, what is their significance and how they are exploited by the fraudster. He also explores both the tactical and strategic approaches that you should adopt to help detect and reduce fraud, including detection techniques and the use of technology.

ISBN: 9781138270060 | £43.99 | August 2016



Fraud: The Counter Fraud Practitioner's Handbook looks at fraud investigation methods and explores the practical options for preventing and remedying fraud. An effective fraud and financial crime strategy involves intelligence and prevention, criminal and civil legal procedures, and asset recovery, all of which may involve investigators, internal auditors, security managers, in-house and external legal counsel and advisors.

ISBN: 9780566088322 | £175.00 | April 2016



Some have estimated that healthcare fraud in the United States results in losses of approximately $80 billion a year. Although there are many books available that describe how to "detect" healthcare fraud, few address what must be done after the fraud is detected. Filling this need, Charles Piper's *Healthcare Fraud Investigation Guidebook* details not only how to detect healthcare fraud, but also how to "investigate" and prove the wrongdoing to increase the likelihood of successful prosecution in court.

ISBN: 9781498752602 | £55.99 | March 2016

Chapter 5

Thinking like a thief

How to out-think the fraudster and predict where your organization is being defrauded

> I may be on the side of the angels, but don't for a second think that I am one of them.
>
> (Sherlock Holmes to James Moriarty, BBC Television Series, 2012)

Seeing the ghosts of past, present and future fraud and corruption[1]

The aim of this chapter is to provide you with a menu, consisting of three important recipes in the form of an appetiser, a main course and a dessert, which will enable you to assemble one of the most realistic 'pictures' of the types of fraud and corruption which can afflict your organization in the future, and, most probably in some cases, have been, or are, already taking place but have not yet been discovered.

It is, of course, possible, using today's technology, which enables virtual meetings which are almost as real as face-to-face encounters, voting buttons and shared documents, to perform the whole process in a way that nobody has to physically meet any business associate. It is also technically possible today for a group of good friends to sit down to a virtual dinner together, share the same meal and have a good dinner conversation. But most of us would agree that there is still something special about the experience of meeting real people in

real life. Either way, I would recommend that when doing the exercises in this chapter, for the first few times, at least, people should to be in the same physical space, and paper, pens, flipcharts, whiteboards and body language should take precedence over technology.

Typically, the menu in Table 5.1 (excluding the synthesis) would take about three or four hours to accomplish.

These recipes are extremely useful and have been used by leading fraud detectives for over 30 years. They are based on using knowledge we already have, brainstorming with an inverted mind-set so that we can mirror that of the potential fraudsters and criminals, and a clear-thinking 'blank-piece-of-paper' approach, free from preconceptions and denial.

The name of this approach, 'think like a thief', was coined in the 1970s by Michael J. Comer and Martin Samociuk (two highly experienced and maverick practitioners, whom I was fortunate enough to have as my teachers), who saw that corporate fraud was rife but not being discovered. Applying the 'lateral thinking' ideas propagated by Edward de Bono, the two experienced fraud investigators and maverick authors of books on fraud and corruption, developed the seeds of an exciting new methodology which gave people working in organizations the chance to put themselves in the shoes of the opposition, to really see how they would attack. This method was new to fraud and corruption, given that the standard methods (which are still dominant today) are still

Table 5.1 How to understand and assess the risks of fraud and corruption in your own organization

	The à la carte menu
The appetiser (Recipe 1)	Warming up the audience to be able to recognize that fraud and corruption is taking place
The main course (Recipe 2)	Using the 'think like a thief' method to reveal the invisible fraud and corruption which is already happening (or could very easily happen)
The dessert trolley (Recipe 3)	How to develop a realistic and living profile of the most significant methods of fraud and corruption which affect you and your organization.
The aftermath	Not a recipe as such, but more instructions on how to use the output from everything to create a first-draft *unique* fraud and corruption profile of your organization. Often this session is done in a small group after the main guests (i.e. most of the participants) have departed.

very much checklist-based. However, the idea is not new at all. Trying to out-think the enemy is an ancient concept and is relevant in many arenas, ranging from warfare to modern-day football.

Some people ask, when they are told to think like criminals, whether the method itself is dangerous and wonder if they will become criminals. This is a natural question to ask but experience shows that it is rare.

Example 5.1 The trigger

Many years ago, Martin Samociuk gave a 'think like a thief' workshop to a group of Scandinavian auditors and IT security specialists where they were encouraged to identify loopholes in the system which could be exploited by fraudsters and hackers. The organizer of the workshop, a young and enthusiastic computer auditor, was very pleased with the response and results.

Years later when involved in investigating for a Scandinavian bank, a simple fraud took place where the same organizer of the seminar, now working as an IT auditor working for the bank, had gained access to client accounts and transferred several small sums of money to his personal account (also with the same bank). It was one of the simplest frauds to investigate and prove and the person involved confessed almost immediately.

What had happened between the seminar and his act of theft from the bank, was that the young IT auditor had been involved with a young lady, whose relatives were mixed up in low-level organized crime. She was also, unfortunately and previously unknown to the IT auditor, a drug user. At some point in the relationship, her brother had 'leaned on' the IT auditor to find a way to procure ever increasing sums of money for her to buy drugs. It seems that 'blind love' was the motivator, and the seminar he attended a decade previously had very little to do with it whatsoever, other than making him think once before acting.

Most fraudsters are leaps and bounds ahead anyway, so think like a thief (or 'TLAT') just allows honest people in organizations to catch up a little.

Before diving straight into the recipes, it is useful to examine why this method works so well and some of the reasons why it has not been used enough in the past.

Why don't we see fraud and corruption normally?

In truth, there is and should be no shame in being cheated or duped. It happens to most of us regularly, often without us realizing. In today's fast-moving world, being cheated or scammed does not mean you are stupid or have something to be ashamed about. It happens to the best of us. Also, there are few paragons of virtue around. Those people whom we hold in high esteem for doing admirable deeds one day, the next can do fraudulent acts often without being 100 per cent sure that what they were doing was fraud.

And there are few pathological fraudsters and corporate psychopaths, although they do exist. Most people who commit fraud are really 'fraudsters for life'. As discussed previously, almost everybody could potentially be a fraudster. And at the risk of sounding a little flippant, one of the catch phrases of Michael J. Comer was 'shit happens and so does fraud'.[2] Or as we put it a little less bluntly, 'fraud and corruption happens'. There will always be some outsiders, such as suppliers, customers, agents, consultants and opportunities who are deliberately trying to do something unethical for their own personal benefit, and maybe they are helped by insiders. Or if we are a bit unlucky, insiders do it on their own.

On the contrary, when we read about fraud and corruption in the newspapers, we feel shock horror, whether it is the latest news about a former FIFA president, billions of dollars syphoned off by an oligarch or president or the latest collapse of a major corporation or small country (such as the financial collapse of Iceland in 2008).[3] Deep down, we probably all know that a lot of this goes on, a lot of the time and what we read about is just the tip of an iceberg which may or may not be uncovered. But we are, I hope, all realistic enough to realize that if we don't see the rest of the iceberg, it has not just magically disappeared.

The paradox, that we know fraud and corruption is normal, but like to think of it as exceptional impairs our ability to recognize it. The key lies in the use of the word 'risk'. Call fraud and corruption a 'risk' and there is that wonderful get-out clause which allows you to say it 'may' or 'may not' happen. I have a colleague who would argue that it must be called a risk even though he knows it happens all the time. But my colleague would also say that 'death' is a risk, even though all of us (even the Dalai Lama) would say that death is inevitable.

Most annual reports and financial statements of large organizations and corporations now include a section with the title 'Risk' or 'Risk Management'. Like external audit reports, the 'risk section' tends to be quite long and written

in small print and is probably one of the least-read portions. But it ticks all the right boxes and covers all the right topics related to risks that the organization could face. It feels as if someone has written a section of the annual report which just has to be there.

What is almost always glaringly obvious as missing is a section which details all the different methods of fraud and corruption which are probably taking place. Is the risk report meaningful? The answer is probably yes, but not in the context of fraud and corruption.

Example 5.2 Fraud: severely hyped but rarely found

A government-owned scientific research centre did its own research and commissioned research as well as assessing applications and awarding grants. The organization had in total a research budget of around £500,000 and literally hundreds of on-going projects. In the 178-page annual report, the word fraud was mentioned 17 times in total. In all but one case, the context was to say how seriously the organization took fraud and how it recognized fraud or how important it was to report fraud. The report went on to say that risk analysis was continuously being done to assess the risk of fraud. Towards the end of the report, buried in a note, was the statement: 'In the financial year 2017, two frauds were discovered, the associate loss of which was less than £1000 in total.'

This example is quite typical of almost every organization which is required to describe risk or fraud risk in its annual reports. Fraud and corruption is rarely mentioned and, if it is, it is usually in the form of a disclaimer: 'to the best of our knowledge we do not believe that there have been any significant instances of fraud', etc., or as an obscure footnote.

Because of this inherent desire not to see fraud for what it is, there is a tendency to not want to see it, or to avoid mentioning it, because of its negative connotations. So, although we know there is a lot of it around and most probably affects us too, putting it back on the agenda is no easy task. And given today's serious under-reporting of the risk, it is unlikely that many people are going to be pleased if suddenly the risk reports lurches from 'we don't think there is a major risk of fraud and corruption' to 'it is normal, and the impact is x per cent of our expenditure budget or revenue'.

Putting fraud and corruption back on the agenda

Once we can recognize the challenges, it is easier to bring the fraud and corruption words back in. The clue is to recognize that fraud and corruption is happening under our noses and, at the same time, see the challenges and obstacles that prevent us from seeing it. Here are some rules to help you do so:

- *Be realistic rather than naïve*: This is nicely summed up the Sherlock Holmes quote in the epigraph, which can be interpreted as: 'We understand how fraudsters think and how they act, in order to be able to predict what frauds are already happening to our organization, without actually becoming a fraudster.' At first, this might sound like a tall order, but as Professor Dan Arielly recognizes in his famous talk, 'The honest truth about dishonesty',[4] most honest people are able to cheat at times and find ways to discount (or rationalize or normalize) this, so they don't see it as cheating. So, all we need to do is tap into those reserves of energy that we all have. By recognizing the potential fraudster within us all, we are also taking steps to bring it under control, i.e. taking precautions that we will not become a fraudster ourselves.
- *Think laterally*: The second, and related, rule is to think outside of your own comfort zone, also known as thinking outside of the box or thinking laterally. Don't be constrained by what can't be done, but think what can be done[5] ('carpe diem' in Latin or seize the day). The TLAT method allows you to tap into that creative side which we all have, use our fantasy and not feel boxed in by either predefined beliefs or our circumstances.

Example 5.3 Fraud awareness

A fraud awareness workshop was held for a group of people working in the Finance Department in the head office of a multinational corporation. The participants were each asked to think, if they were dishonest and had an urgent need of cash, how they could defraud their own organization, but wanted to avoid being caught. Many of the participants found the task quite easy and came up with the seeds of rather simple and powerful methods. But one lady said she felt she was 'too honest' to even be able to think this way. When asked what her actual job was, she replied that she was responsible for executing payments, many of them in the region of tens of millions of dollars.

At the risk of sounding simplistic, I would like to kick off this chapter by stating the obvious. You won't understand how fraudsters think by being appealing to your fundamental belief that you are always 100 per cent honest. Somehow you must allow yourself to walk in the shoes of your enemy. Also we need to ask ourselves the question: what is the difference between the unthinkable and the unknowable?

Allow yourself to think the 'unthinkable', even if it means pushing yourself to imagine scenarios you would rather avoid

It is just human nature that we do not like to imagine the worst case because it is something we cannot bear to think about. To make it a bit easier to think the unthinkable, we can ask ourselves questions such as:

1 Would a well-paid, well-respected CEO commit fraud and corruption if they could find a way to do it and not get caught?
2 Would an external business partner or supplier like to make more money from their clients if they could, even if it meant the client paying a little bit more than they had to?
3 Would a respected doctor who already had a comfortable life, but feels he or she does not get the respect he or she deserves in society, start to put some of his or her most hypochondriac or unnecessarily depressed patients out of their misery (by humanely killing them), provided he or she did not get caught?

Most of us could answer yes to the first two questions. Certainly, not all but many people, at the top of their game, feel that they are worth it and often worth a bit more. Some of these people are willing to do whatever it takes to get more money even if this means doing something unethical. And for question 2, everybody 'in business' would say it's about maximizing your returns – it's just if you maximize them too much, especially in the short term, you can end up doing something unethical.

And, as discussed in Chapter 2, we can accept that almost everybody who does something which either before or after they see is unethical, will attempt to rationalize their actions. The excuses are: 'I was worth it'; 'this is business, not fraud; the price is whatever people can pay'.

But what about the answer to the third question? Along with judges, doctors occupy a place high up in society. In my own personal experience, my father

was a consultant in the National Health Service, and prior to that worked in India, he was always talking about fraud in the health services: whether it was (in India) professors taking bribes for admissions (the reason he chose to leave India), or later on doctors and dentists who would either use public resources for private treatment, accept too much sponsorship from pharmaceutical companies or medical equipment suppliers and thereby were influenced, or just simply cheat on expenses. Doctors are, after all, human. But this is fraud and humans can commit fraud. But a doctor who deliberately kills his or her patients (in spite of taking the Hippocratic Oath) sounds more like a monster. One of the most powerful and concise, albeit macabre, examples is the case of Dr Harold Shipman (see Example 5.4),[6] as it illustrates both our unwillingness to think the unthinkable and (if we are not willing to think the unthinkable), our inability to notice the warning red flags. Just like most customers, suppliers, agents, consultants and employees are decent, basically honest people, the same can be said for doctors too. But there will always be potential rotten apples and we should not be naïve.

In the same way, one of the greatest obstacles to detecting fraud is that most relatively honest people find it difficult to believe that a colleague, manager or third party is dishonest – that is the nature of people. In a normal, safe and nurturing working environment, people do not want to believe that something terrible is happening – whether it is fraud or some other shocking event.

Example 5.4 A case of the unthinkable

No book on fraud and corruption would be complete without a horror story. The following true tale illustrates just how serious the consequences can be when red flags are overlooked.

In July 2002, an inquiry in England concluded that a doctor called Harold Shipman had murdered at least 215 of his elderly patients during routine home visits, by injecting them with lethal doses of drugs. He had carried out these activities over several years and, to the outside world, he appeared to be a nice, family man, and a respected doctor. The reality was that he was a killer. Today, the question continues to be asked why no one reacted to the tell-tale signs, including abnormally high death rates on his call-outs or exceptionally high order rates for certain drugs

which were eventually used to murder his patients. The reason Dr Shipman managed to get away with it for so long was because the caring, honest people around him could never have imagined or believed that something so terrible was going on. As a result, nobody looked for the red flags.

Why was Shipman not discovered until he had killed hundreds of his patients? It was a classic case of blocking out the unthinkable and not accepting the truth that was staring us in the face. Shipman was a lone doctor seeing multiple patients who were often elderly and maybe a little fed up or suffering from something. He had lots of drugs which in certain quantities would be lethal. He had the perfect opportunity.

As for motivation, it was not money this time. Shipman had a comfortable enough life. However, he could simply have been bored, or felt that he was not respected enough. Whatever we speculate, he certainly had the motivation and as many experts who have analysed the case note, his overarching motivation was that he wanted to 'play God'. If we search the darkest deepest regions of our souls, who can say they would not also like the chance to play God from time to time (it's like the stranger on the bus, who says 'If I was in charge, I would . . .').

And as for Shipman's rationalization, he could have come up with a number of reasons including, 'they were not happy with their lives, so he helped them end it, humanely' or 'he was putting them out of their misery' or, stretching it a bit, he was saving the National Health Service money, in avoiding long and expensive treatment in the future. However ludicrous you may think his rationalizations were, the point is that he believed them.

The facts are that, whatever his motivation and reasons, a well-loved doctor killed over 200 of his patients, people who went to see him because they trusted him (and should have too). What happened was that collectively the system of recognition and detection failed. And this is what happens again and again with fraud and corruption. We often don't see it until it is too late. But if we can find a way to see it, to predict it, then we can learn to spot it. The key is to learn from Shipman and think the unthinkable.

To turn the tables on fraud and corruption, we need to be pre-emptive using two powerful techniques:

1 Stimulate people working in organizations to start to view their own organizations from the vantage point of a potential fraudster (using the menu in this chapter).
2 Follow the money and find fraud and corruption early (part of which is covered in Chapter 4 and will be explored further in Chapters 6 and 7).

It is often said that an outsider can see the organization more clearly. However knowledgeable internal people, who can free themselves from any biases, will see even more.

Recipe 1 The 'appetiser': preparing to be able to think like a thief and see fraud and corruption

I have called this recipe 'the appetiser' because you should think of it as a way of warming up a group of people in an organization to recognize that fraud and corruption happens and, despite even the most stringent controls and security measures, people who are motivated will always find a way. Think of Recipe 1 as a warm-up exercise which precedes the main event where people start to brainstorm which frauds are the most likely ones to happen in their organization. I would recommend that the typical time needed for this recipe is in the region of 15–45 minutes, depending on how much the participants wish to engage in the preparation.

Ingredients and tools

Before starting, you will need:

- *A group of reasonably motivated people who work in the organization.* This can be a cross-section of people from one department, from across the whole organization, or also people working with one or two key processes in the organization. The key to the selection is that the people who are attending should feel that they 'know' the organization enough to be able to recognize (with some coaching) how it could be exploited. Where possible, ensure that diversity in gender, age and cultural identity is represented in the small cross-section. The people who know the organization best are the people who work there! The size of the group could vary from as few as eight to as many as 40, although the higher the number, the more time will be necessary.

- *An invitation to participate* tells the people that they are joining a fraud and corruption awareness session which is going to be different and where their participation is invaluable.
- *An airy room with a large whiteboard or flipchart.* The room should be set up with tables for four or five persons or cabaret-style, as is it is often described. Try to avoid people having laptop computers plugged in or phones on the desk, as it just creates unnecessary clutter and distractions. Ask them to turn their phones or pagers off.
- *Coloured pens* to draw on the whiteboard or flipchart.

One note of caution before starting: senior management should support the brainstorming session but not try to dominate it. Management can participate actively, but in small numbers, and at the same time they should encourage their staff to think critically and want them to see the iceberg below the tip. From the outset, they should foster the mind-set. 'We want to find fraud early and we want to be ahead of the game'. That would be the sort of message that management need to genuinely send.

Method

Open the brainstorming by telling the participants why they are there and what you are going to take them through. Tell them this is not a session about finding fraudsters among the staff, but today they are going to identify how external fraudsters can exploit and attack the organization. Depending on the room layout, make sure people are sitting close enough to be able to work in twos or threes. Let the audience know that quite soon we are going to run a 'think like a thief' session. And if some of the audience look a bit startled or worried, then reassure them that they will receive expert guidance and they are not going to become criminals.

Before launching into the TLAT exercise, you should spend 10–15 minutes warming the audience up or getting the audience into the zone. The aim is to dispel any illusions that fraud and corruption is not real and is not something almost everybody is involved in. This should be done using a short awareness session:

1 Define fraud and corruption for the purposes of this workshop as 'anything deliberate and unethical, done by anybody, inside or outside, which causes loss'. Define loss, for example, as the sum of 'loss of revenue and profits + damage to reputation and brand + erosion of the organizational culture'.[7] You can ask for a show of hands by asking the question, 'Using this

definition, who here might have seen something which looks like fraud and corruption?'

2 Ask the audience what they believe is the total cost of fraud and corruption (repeating that you mean 'everything deliberate and unethical done by both insiders and outsiders'), giving them the model of an organization with sales of €1,000,000. Remind the audience that, by cost, you mean *all* costs, which include loss of money or value, damage to reputation and erosion of the organizational culture. Just give them the choices below and ask them to make their best intuitive guess at the total cost which can be quantified (writing up the categories on the whiteboard):

€0–€100,000
€100,000– €1 million
€1 million–€5 million
€5 million–€7 million
€7 million+[8]

3 Give the audience about 60 seconds to respond and then ask for a show of hands trying to go through this as quickly as possible but still ensuring that everyone does have an opinion and then write up the answers. The results almost always show from an intuitive exercise like this that people believe that the average costs of fraud and corruption is around 1–5 per cent of sales. If you like, feel free to make comparisons with relevant and current surveys and statistics which are constantly being updated but put the value in a similar ballpark.

4 Then ask the question: 'Who commits fraud and corruption?', starting with the factors as to why fraud and corruption can take place. Explain that there are three fundamental factors underpinning why fraud and corruption happens.[9] Tell them: 'You would never be able to do fraud if you had no opportunity. And you would never be able to do something deliberate and dishonest if you had no reason to and you absolutely were not motivated. And finally, you would only do something bad if you were able (maybe only after the fact) to justify to yourself at least your actions.' This third factor is known as 'rationalization' and was covered in more detail in Chapter 3.

5 Deal with opportunity first. Keeping in mind the true cost of fraud and corruption, which you have established, ask the question, 'Who has the greatest opportunity in money terms and per incident to commit fraud? Is it, in general, people near the top of an organization or is it people near

the bottom?' (Almost always, you will get the answer that it is people near the top but there should be some hands which believe it is people near the bottom.)

6 Then say that we are going to deal with motivation next. Ask the question, 'What do people with loads of money want most?' The most common answer is in fact 'more money'. Then you can comment, 'Big people, big frauds, smaller people, smaller frauds.'

7 The last part is asking the question, 'Who then are the criminals?' What we are trying to establish here is that most people in the room have the opportunity, have some greater or lesser degrees of motivation, and are typically able to rationalize their actions when they need to. However, this is quite a difficult and sensitive part of the warm-up process and needs to be practised in advance before trying it out on a live audience.

In order to emphasize that anybody, with the right opportunity, motivation and rationalization can commit fraud and corruption, do the following exercise. Ask everyone in the room to put their hands up and keep them raised. If they answer 'yes' to even one of the questions, then they should put their hands down. These are typical questions, although you can vary the nature and number of questions depending on the audience:

- Who has at some time in their life written an amount which they believe is just a little too high on a personal insurance claim?
- Have you ever, and please be as honest as you can, not declared all your income, even small amounts, for tax purposes?
- Have you paid someone to do work for you, like a builder, electrician, cleaner or plumber, where you paid them in cash and you did it because it was simpler without an official invoice being submitted?
- At some time in the last ten years have you avoided paying a bus or train fare?
- Have you driven more than 20 km over the speed limit, noticed your own speedometer and then not 'done the right thing' and reported yourself to the nearest police station for dangerous driving?

Turn your back on your audience when asking the questions. Feel free to vary the questions. You can find additional questions in the format of an online game called 'How far can we bend the rules?' at www.fraudacademy.hibis.com. This exercise usually creates laughter in the audience as most people have lowered their hands after five questions. However, it is important to practise

this, and at no time be judgemental, as it is most likely that you too fit into the category, 'I am also a fraudster'. The purpose of this exercise is so that you can finally say 'now we are ready to think like thieves' because we can now see that being a fraudster is just human nature.

Helpful hints and tips

Preparation and the warm-up exercises above require practice and you will improve your presentation and facilitation style with experience. Remember you are not holding a lecture as such. Keep your presentation and style always light, not flippant, but add some humour at times. Participants need to feel involved but also relaxed from the start. If you can get them interacting and talking very soon, then they will be much more generous with their ideas when they have to brainstorm and think like a thief in recipe 2.

Recipe 2 The main course: using the TLAT approach to make the invisible visible and recognize fraud and corruption

This recipe is the essence of thinking like a thief. It requires more time and sensitive handling of the participants. They now should be in a frame of mind where they recognize that fraud can happen and probably does happen in most organizations, they realize that the total cost of fraud and corruption is 'a substantial chunk of change' and they recognize that nearly everyone can be a fraudster. These are perfect conditions to stimulate them to start thinking like a thief.

Typically, around 45 minutes should be allocated to this stage, allowing you to develop a fairly diverse and relevant list of methods of fraud. However, the exercise can be longer, but it is very likely that in this case you keep it focused and write down all the methods.

Ingredients and tools

The tools and ingredients are essentially the same as for Recipe 1. In addition, each participant should have some sheets of paper and a pen. One person should be nominated (by the group) as a scribe, who can write down all the methods which are generated in freeform text. (Alternatively, and this works well in sessions with larger numbers of participants, have an assistant who will mainly focus on writing down the methods.)

Method

1 Tell your participants that you will be giving them an exercise which we call the 'five-minute fraud manager'. Write up on your whiteboard the following:

   You can BE anybody you like outside or inside of your organization. Then, think of a fraud where you need to be able to get at least €10,000 from your organization, and not get caught. Ideally pretend you are an outsider who does it alone (although you could be an insider but ideally not you!). Look for the loopholes in the system, i.e. the opportunity. Be motivated and driven and think of a method where you will not be caught!

2 To be sure that everyone is following, repeat the instructions and explain that this exercise is about your own gut feeling, pushing the limits and putting yourself in the shoes of someone who is determined to commit fraud and corruption. Explain also that the best results come when you think of being someone who is highly motivated and has a big (in terms of money) opportunity. In the best situations, people are asked to make notes of their method so that they will remember it.
3 Ask the participants to think in complete silence for 2 minutes and then ask them to write down some bullets describing who they are and what they would do.
4 Then ask the participants to pick a partner in the room and tell their method to them (and vice versa). But give clear instructions that the person who is listening is only allowed to constructively criticize the method. It would be tempting to say something like 'this method would not work because . . .' because people like to trust in the defences rather than admitting how easy it is to be exploited. So, it's important to encourage the participants, for this exercise, to help each other improve or 'sharpen' their methods rather like a whetstone is used to sharpen a knife. It's fine to identify obstacles as to why a method might fail but then it's important to try to identify how to overcome or circumvent these obstacles.
5 The aim of the brainstorming and feedback sessions is to generate as many methods as possible. Encourage each pair to refine their methods and then jot them down in the refined form.

Presenting what you find

After around 20 minutes of this brainstorming, ask for feedback from the audience. Depending on time, ask each pair to present their two methods

and then listen carefully. Ask them to present in, say, 30 seconds in the format 'I would be Mr X who is . . . and I would do this . . .'. It's important to listen to *all* methods without judgement. People should not say 'my method is the same as the person earlier' but should be encouraged to describe their method, focusing on the small differences and nuances. And it is important to write down all the methods. This recipe should be an 'ideas generator', allowing people to think creatively about how the organization can be defrauded. An experienced facilitator can often generate 30–40 methods in a one-hour session.

Helpful hints and tips

The TLAT workshop, as this is called, is a very powerful technique to help change the mind-set of a group from one of 'denial' or 'I don't believe we have fraud in my country or my organization' to one of openness to that fact that it probably is very likely. However, like Pandora's box, the results need to be contained. Below are some tips and advice based on the experience of running these sessions hundreds of times:

1 Do not be judgemental and try to foster a spirit where no one in the room is either overly critical of anyone else, inside or outside the room, or judgemental. The idea is to 'enjoy' thinking like a thief.
2 The value does not need to be €10,000. It can also be more (or less) but try to pick a number which is not trivial.
3 Sometimes people when they think about a method, want to tell you instead, in the third person about something that already happened, which others in the room know about. You want to avoid this. You should try to remind the person that you have asked them to put themselves in the shoes of someone on the outside or inside who will commit fraud and then describe it using the 'I' pronoun. For example, 'I would be a supplier and I would invoice for services and add a 20 per cent mark-up which would not be noticed, because I would be the supplier on Project X which has such a high budget that the project manager, Mr Y is not looking at the costs in detail but just signing off based on reasonableness.'
4 If someone says, 'Will I become a criminal?' or tries to say that this method is dangerous, you can easily counteract this by saying that the real criminals are several steps ahead and all we are doing here is catching up.
5 Try, when listening to people's methods, to help them 'build' the method. Your role is that of a facilitator where you want to get the best (or in

this case the 'worst'!) out of people. So, if someone has a method which is 'half-baked', try to help them develop it by asking questions, or even allowing another participant to help them develop it. You can always say that 'Fraud was not invented in a day. What you are looking for are the seeds of an idea.'

6 Quite often there are people in the audience who wish to talk about possible frauds that they have seen but never reported and, when talking about their method, use the feedback session to point fingers at parties or people. This should be avoided. Say you are looking for methods and stories without reference to specific parties and people at this stage. However, do say that you can talk with them later. It is important that you do genuinely set aside time for this if needed.

Sometimes people get stuck and say they are unable to think of a method. It is usually obvious which people don't wish to speak. I have found that they typically fall into three categories:

1 People who simply feel they are too honest to be able to commit fraud. In this case, you need to first commend them for their honesty, and then ask them the question: 'If you had access to huge sums of money but were too honest to misuse them, what would others have to do to you to coerce you into doing something dishonest?'[10]
2 Senior management who feel that, for one reason or another, that fraud does not happen in *their* organization. Maybe it's because they have had so few incidents, maybe it's because they have had clean external audit reports for years and believe that external auditors find fraud, or maybe it's because the system of compliance, risk management, audits and policies has made them believe that fraud cannot happen, or maybe they are just idiots. Who knows? One way is to give them the 'dishonest chair scenario' described in Example 5.5.
3 People who are already involved in something and who are feeling uncomfortable. This is quite a difficult category to handle and needs to be done very sensitively. See Example 5.6.

Holding a TLAT workshop requires some experience and it needs to be handled sensitively because situations as in Example 5.6 can easily arise. In other cases, people who have wanted to speak up but for one reason or another have not done so, can tend to talk about real events. In all cases, the situations need to be managed in a calm and collected way.

Example 5.5 If there was a dishonest person in your chair?

In one TLAT session for a senior management team of a large IT company, the nine managers sat around a table smiling confidently. The methods that they came back with were almost the same. They felt that they had very good controls and procedures but felt that some of their employees, who were travelling a lot, could cheat on their expenses. There was no talk about senior managers working in collusion with suppliers, individual client account managers overbilling their customer for services that they did not really require, or similar major fraud. At this point it became apparent that this senior management team believed that the company had no fraud, or very little, because they saw themselves as 'good' people.

Each one was then asked the question, 'If there was a dishonest person in your chair, what could he or she do?'. Going around the table it was as if the floodgates had opened and method after the method simply poured out.

Example 5.6 Hard-pressed to think of anything, or . . . ?

At one session, with around 25 people from a local authority participating, one gentleman did not engage with a partner, when asked to think like a thief. When it came to the feedback session, with arms folded, he said he could not think of anything. A little curious, I asked him what his job was, and he said he was responsible for purchasing PCs and other IT equipment for the whole of the organization (an organization where over 10,000 people worked). However, I felt even though it seemed strange that he could not think of a method, it felt more appropriate to politely accept that he did not want to contribute at this stage and move on to the next person but I made a mental note that it could be interesting to speak to him on a one-to-one basis later.

This was not necessary because, at the end of the workshop, the gentleman approached me to say he felt very uncomfortable as he himself was the joint owner of a company which sold computer equipment, which was run by his brother, and he knew that this company had been a sub-supplier to one of the local authorities' major suppliers of PCs. In other words, during the seminar it had dawned on him that he was probably involved in some sort of fraud or conflict of interest and had simply not realized it until now.

These workshops are a very powerful way to both recognize fraud and corruption, discover where it is likely to happen, and crystallize the methods into a fraud and corruption profile (as per the final recipe in this chapter). However, it needs proper preparation and some experience to do it well.

Recipe 3 The dessert trolley: how to start developing a realistic profile of where fraud and corruption is happening

The aim of this recipe is to produce a first draft of a fraud and corruption profile for your organization. By a fraud and corruption profile, what we mean is a sort of dynamic map of all the methods, which are ranked according to a combination of how likely each method is and what the impact of each method is. This recipe builds on the work done in Recipes 1 and 2 and takes into consideration the methods generated at the end of method 2. What we do here is to generate more methods in a systematic way, most likely those which are the most relevant to this particular organization. The typical time needed to generate and document the methods as well as do an initial ranking would be around 1½–2½ hours where most of the time the participants would be working in groups. After this, the synthesis and evaluation, which are done in a smaller group, can take a few hours.

Ingredients and tools

The same participants from the workshop in Recipes 1 and 2 above, but now working in groups of approximately four around a table. Pens and paper and put a simple form on each table showing Figures 5.1 and 5.2. Figure 5.2 can be photocopied as many times as necessary. The form is deliberately simple. Each group should also have the hand-written notes of different methods that they generated in Recipe 2.

Fraud and corruption risk brainstorming using the TLAT methodology

What do we value in our organization?	**Who are the potential fraudsters?**
_____	_____
_____	_____
_____	_____
etc.	etc.

Figure 5.1 Capturing the results from a think like a thief brainstorming session: a suggested template

Method of fraud and corruption	Likelihood		Impact		
	Vulnerability	Frequency	Profits/Value	Reputation	Culture

Figure 5.2 Assessing the likelihood and impact of fraud and corruption: a suggested template

Method

Explain to the participants that now for 45 minutes or so they are going to repeat Recipe 2 but in a structured way to generate as many realistic methods of fraud and corruption as possible. What you would like them to do is:

1 Nominate one person as the group's scribe, preferably someone with legible handwriting.
2 Think of all the things that they feel are of value in their organization (or if they prefer they can think of 'assets' in the widest sense). This could include everything from 'money' to 'a nice organizational culture'. Try to come up with at least 10 completely different types of value in just 5 minutes of brainstorming. Write this list on Figure 5.1.
3 Then spend 5 minutes thinking of all the different groups of people (from professional criminals to dishonest management!), the 'opponents', who could defraud or harm your organization in an unethical way (for their benefit). Once again, use just 5 minutes on this and try to come up with a list of around 8–10 different opponents. Then brainstorm as many methods as possible where people can do something unethical which causes harm to something of value in your organization. Write them down on Figure 5.1.
4 Try to generate at least 10 methods in 30 minutes and write a few lines about each method in the left-hand side of Figure 5.2.
5 Once you have generated at least 10 different methods, then write H (for 'High'), M (for 'Medium) and L (for 'Low') in any of the boxes on the right

next to a method in Figure 5.2. The heading should be self-explanatory, but you may want to point out that the reason that Likelihood is divided into 'Vulnerability' and 'Frequency' is that 'Vulnerability' measures your feeling as to how possible it is to commit this method, whereas 'Frequency' measures your feeling as to how often you think it happens.

6 Before starting, remind participants that they should not get stuck in lengthy discussions. The atmosphere should be one of 'anything goes' and 'nothing is a stupid idea'. And ensure that the groups write things down.

Serving suggestion

At the end of 45 minutes, participants should have done enough. Say, pens down, ask if it is OK to collect the forms and give the participants a well-deserved break. Read the forms and select (ensuring that each group is recognized) some 'highlights' such as some particularly interesting types of value and 'opponents', as well as some particularly interesting methods. Feed this back to the participants, thank them very much for their time and ask them for some feedback and comment on the workshop.

If it is appropriate, do also explain to the participants that they will be getting more feedback in different ways, but for now their creative energy and output are going to be reviewed and synthesized.

Useful tips

One typical question from this sort of session is 'what happens next?' You can answer this by saying that now you (and a small group) will review the results and see if any really obvious methods which are important have been missed. Usually because our organization is rather unique (as all organizations are), then it is likely that 90–95 per cent of the most important methods have already been captured in this workshop. Synthesizing the results of the raw brainstorming into a fraud and corruption profile of the organization with the most serious frauds at the top, is something which is done afterwards. Under the right circumstances, I believe that this profile can be shared with the participants of such a brainstorming session but one also has to consider confidentiality.

Sometimes in the brainstorming, participants get stuck or hung up on particular issues. Keep reminding them that this is a free-thinking brainstorming, and that they should not get obsessed with details and technicalities. Often the simplest methods work best.

Afterwards: synthesizing the results of the structured brainstorming into a unique first draft fraud and corruption profile

Let's assume that you have run a successful and interesting workshop using Recipes 1, 2 and 3 in that order. The participants have generated lots of ideas, especially during the second and third courses and provided you with a lot of very useful input to help you prepare 'a first cut', or first picture of the major methods of fraud and corruption which will affect their organization. While you can be sure that not every significant method will have been covered or even addressed as yet, what you should be pleased with is that the methods generated are those which are really applicable to that organization, and are recognized by people working inside as things which could really happen. In other words, what you will be developing will be a living document which is unique to their organization.

Immediately after the participants have departed, ensure that you have collected all the output, including any views on fraud and corruption which came out of the 'appetiser' session, methods of fraud and corruption which came out of the TLAT exercise in the second course, and the completed forms which were distributed in the group exercise, which was course number 3. At this stage it is not crucial who said what, just that it was said and was recorded. Make your own short reflective notes and then, ideally, take a break, which could be a few hours or even a few days. This break is very important as it gives the mind time to think and reflect on all the information you have absorbed during the workshop. When you do return to the material, in order to synthesize it, be aware that your goal is to create a single, balanced and harmonized fraud and corruption profile of the organization.

The five steps you need to go through (either alone or in a small group of two or three persons) are as follows:

1 Review all the methods which have been described (at any stage in the workshop) and try to distil from them between 20 and 40 unique methods which are still very much related to your organization or the organization which you are helping to do a fraud and corruption risk assessment on, but make sure that they do not implicate individuals or named departments as far as possible.
2 Based on the material you have collected (including also the methods), create two distinct lists, in order of importance if you prefer, spelling out what is of most value to the organization and who are the parties and people which could commit fraud against the organization.

3 Sit back and review the methods in the context of the lists of what is of value and who can be the potential opponents. Think of *your* organization. Then ask yourself the question: 'What are the most obvious things that are missed?' There will almost always be one or two things which have been probably addressed in passing but not described explicitly. Feel free to write these methods down and. if appropriate, add them to the list of methods.

4 Using the participants' own rankings of 'Likelihood' and 'Impact', try to come up with something which represents an informed gut feeling for each method. Table 5.2 is just a guide. The most important thing you need to do is be consistent in your thinking and application of the categories High, Medium and Low (as the participants were asked to do in Recipe 3).

Table 5.2 Ranking of the measures

Measure	*What the measure means*	*Ranking (High' (5), 'Medium' (3) and 'Low' (1)*
Likelihood	Vulnerability	How possible is the method?
	Frequency	How often do you think it is going to happen?
Impact	Value (or profits)	In relation to the organization, how bad would it be if the method happened once? What would be the impact on profits or value?
	Reputation	In relation to the organization, if the method succeeded just once, what would the reputational impact be like?
	Organizational culture	If the method happened just once, what would the impact be on the organizational culture (including, for example, trust among employees and colleagues)?

5 Once you have allocated 'H', 'M' and 'L' to each of your methods, you are then in a position to do a basic ranking. The purpose of the ranking is to identify those methods which are highly significant, i.e. they are real and could have a very high impact, or they are real but have a low impact but happen all the time, or some combination of the two. A simple but effective way to do this is to use a formula where you allocate the numbers 5 to 'High', 3 to 'Medium' and 1 to 'Low' which corresponds to the

likelihood and impact factors, thereby creating a Fraud Risk Factor for each method as follows:

The Fraud Risk Factor = (Vulnerability + Frequency) multiplied by (Value + Reputation + Culture)

6 Then re-order your table of methods in *descending* order of Fraud Risk Factor.

In this very simple but effective way you have started to create a realistic and actual profile of the fraud and corruption which is affecting the organization today or is most likely to affect it soon. You will have created a first draft which will be subject to a lot of debate and refinement as well as being challenged. However, you can always use the argument that the methods were developed and recognized by people inside the organization and have not been conjured out of thin air or applied theoretically.

Once the Fraud and Corruption Profile has been accepted as a snapshot of the major fraud and corruption threats facing the organization, then it can be used to focus on the most important fraud and corruption methods in awareness training and swift and effective action can be taken to close loopholes.

Example 5.7 Closing the gap immediately

In one session with a major treasury department of a financial institution, one of the top methods identified showed that the back-up payments solution, should there be a system failure, was highly vulnerable to attack because nobody had identified that anyone, including outsiders, could send payment instructions if they had just a little extra knowledge from the inside. Once the method was recognized in the workshop, the CEO insisted that immediate action was taken to remove the gaping loophole.

Your Fraud and Corruption Profile is a unique and living document which will need to be continuously updated and improved. The overriding principle should be to keep it simple. But you should not care or even enter into a discussion as to whether a particular fraud risk has a factor of 42.13 or 43.62. The key is whether a method has been recognized at all. Dissemination of the Fraud and Corruption Profile is something which needs to be discussed internally.

On the one hand, it should be an open document as it helps employees provide feedback on which methods are occurring, and also which methods may have been omitted. On the other hand, the ranking itself can lead to the organization being held liable for recognizing the risks but not taking sufficient action to mitigate them.

Finally, be aware that people will see the whole fraud and corruption profiling exercise as 'a fun day out' and part of a training course. If that happens, then there is always the challenge that people will go back to their organization after being on a training course to try to implement what they have learned but may be disappointed. To avoid having to prepare participants for this disappointment:

- Ensure that the senior management team are involved and participate in the workshops.
- Present the result in an authoritative manner and include in the workshops real examples from the organization, or make sure that they are identified and documented during the workshop, and followed through afterwards.

In this way, people will appreciate the validity of the exercise.

Notes

1 Fraud is entrenched. As Professor Peter Jackson, one of my esteemed reviewers and mentors in the academic world remarked, Jacob Marley, who was Ebenezer Scrooge's deceased business partner in Charles Dickens' novel, *A Christmas Carol*, adopted practices which ensured that he would not be defrauded but made other people's lives a total misery! Marley was so greedy that in the novel he appears as a tormented ghost who succeeds in changing the life of his former partner Scrooge, by offering him a path to redemption.

2 Quoted with the permission of Michael J. Comer, practitioner and author of several practical books about fraud and how to investigate it.

3 In a seminar about the financial crash of Iceland in 2008, Professor Vilhaljmur Arnasson, who was commissioned by the Icelandic government to write a report into the human reasons for the crash, commented that while there may have only been a few instigators, there were comparatively many people who saw the signals but chose, for one reason or another, to do nothing. I remember distinctly the catch phrase from this illuminating session being 'the worst people are the good people who do nothing'.

4 See Dan Arielly's 'The honest truth about dishonesty' on www.youtube.com/watch?v=XBmJay_qdNc&t=39s

5 When I was 9 years old, I was selected (most probably at random) with other kids to appear on one of presenter Gordon Burn's first editions of the TV programme *Granada Reports*, with Edward de Bono, the man who coined the phrase 'lateral thinking', which is also known as 'structured creativity'. I remember very little of that evening other than that I was terrible at it and managed to break a lot of eggs in one of the exercises, so much so that it was shown as one of the 'embarrassing moments on TV' on New Year's Eve that year. But what did stick was de Bono talking about lateral thinking and thinking outside of the box and how it's important to think creatively and generate ideas. I am reminded of that evening each time we run TLAT workshops, thinking of how narrow-minded I was as a child (and probably still can be today).

6 For Harold Shipman, see the article in *The Independent*, 26 April 2018. Available at: www.independent.co.uk/news/uk/crime/harold-shipman-doctor-death-serial-killer-gp-mass-murderer-hyde-manchester-itv-documentary-a8323176.html

7 If profits is not a commonly used terms in the organization, one could instead use a similarly appropriate measure such as increased costs, loss of pure financial value, etc.

8 The currency, amounts, and ranges used here are purely arbitrary. But it helps to use numbers which recognizably translate into percentages.

9 As per Donald Cressey's three factors, 'opportunity, motivation and rationalization' as described in Chapter 2.

10 In one particular case, the honest lady who could not think of any methods was working in the 'cash payment' department with millions of dollars per week passing though her function. After just a few seconds, she responded to the question of how someone could get her to behave dishonestly: 'If someone had kidnapped my two beautiful children and there was no other way to get them back other than transfer the money, then I could do it with no hesitation, but I would still be afraid of being caught.'