CAPITA
LEARNING & DEVELOPMENT

# Group Risk

## Security Awareness Training 2010 – 2011

## Fraud Prevention Awareness

CAPITA
LEARNING & DEVELOPMENT

## Table of contents

CAPITA
LEARNING & DEVELOPMENT

## 1. Background

Meet Emma.

“At first, I didn’t really grasp the extent of it … When my credit card company called me to ask me whether it was me who had booked airline tickets over the phone for four flights, it was clear that somehow my credit card had been used without my knowledge. But how? It had never been out of my sight. As the weeks went by, it turned out that someone had my passport, my driving license … Had taken over my bank and savings accounts … and had crashed in my insurance policy. Every day, some other piece of my life seemed to fall apart as I learned of another fraud committed in my name. My whole identity had been hijacked. Of course, I had read about situations such as these, but I had dismissed what I had read. You never really think it could happen to you. But it did happen to me. In fact, it happened to hundreds of others too. And it could just as easily happen to YOU!”

## 2. Introduction

As you investigate the circumstances surrounding the financial crime and identity theft to which Emma has fallen victim, you learn that she recently sold shares through an adviser, Malcolm, who had contacted her out of the blue. He told her that he worked for the share registrars who administered her share holding and since she was strapped for cash, now seemed a good time to sell the shares.

Malcolm already had details of the shares Emma owned. All she had to do was to complete a simple form which he would email to her, and a cheque would be sent to her within the next few days to the value of the sale less his commission. Emma duly received the cheque through the post less a small commission and she was very happy.

Some time later, Malcolm contacted her by telephone again to ask her whether she was interested in buying some shares in a small but expanding company. Emma seriously thought about this, especially as Malcolm had previously been so helpful. However, she decided not to go ahead at that time as she really didn't have the cash to spare. But Emma did begin to wonder how Malcolm had targeted her in the first place. Find out how Malcolm may have come to target Emma.

In this module you will learn that Emma recently sold some shares and visited her online bank account website which the bank had recently re-vamped.

## 3. Searching the internet and responding to telephone calls

Some people believe that so much information about us is out there that we might as well not worry about providing more. After all, our names and addresses can be found in the telephone directory and on the electoral register. When we shop, we give our personal details to trusted retailers on the high street and on-line, including our names, address and credit card details. With closed circuit television cameras on virtually every street corner, supermarket loyalty cards capturing our every purchase, and if we travel in London using Oyster cards, our every journey being recorded, some say that there's little point in us trying to protect our personal information. We live in a world in which anyone can find out anything about us. That some of our personal information is already out there is not an argument for handing over the rest to fraudsters! And there are a number of ways fraudsters actively search to get hold of our personal details to defraud us or steal our identities. Mostly, they find our personal information because we have been careless in publicising details it would have been better for us to keep private. Sometimes, they find it because we have provided it to a company, a shop, an online supplier, and they have lost it or disposed of it without regard to our safety, or have sold it on to a third party that then fails to protect it with any real care. One technique fraudsters increasingly use is to search social networking sites.

**Extract from social networking profile – Emma**

Decide which items of personal information you would advise would be better NOT posted to a social networking site:

1. **Full name**

OK. Your name is one of the most valuable pieces of information you have; yet few of us have names that are unique to us and us alone. Giving out your full name is probably not a risk, though on chat rooms and message boards, it is better to provide a 'nickname'

2. **Date of Birth**

Not OK. As soon as you give out **ANY** personal information additional to your name, you start to provide those with criminal intent the means to hijack your identity and to defraud you. Aside from anything else, often we are asked by financial services firms to provide a memorable date as a primary security question. Many use their dates of birth as their memorable dates. Providing this, gives fraudsters the opportunity to access your accounts. NEVER provide your date of birth on social networking sites.

3. **Post-code**

Not ok. This identifies within half a dozen houses or so, exactly where you live. To keep safe, avoid providing your address and post-code. Providing a general location is usually better e.g. South East London … or if a post-code is required, make one up!

4. **Email address**

OK. This really depends on you and whether or not you want to be easily contacted. Giving out email addresses on social networking sites often results in you receiving huge volumes of spam. Spam can contain viruses and trojan horses which infect your computer. A trojan horse can monitor every keystroke you type. So when you next access your online bank account a fraudster may well have your logon, password and security questions. If you want to provide an email address, set up a webmail address for this specific purpose.

5. **Occupation**

Not OK. When you apply for mortgages, insurance policies, and set up pension funds, you are asked for your occupation. This is another piece of unique information about you which fraudsters like to have.

6. **Place of Work**

Not OK. Your place of work pinpoints you better for fraudsters. It might also leave your colleagues vulnerable to attack.

7. **Partner's name**

Not OK. Partner's names are frequently used by people as passwords to gain access to bank and building society accounts and to internet shopping accounts. Avoid criminals raiding your accounts and hijacking your identity by keeping this information to yourself.

8. **Children's names**

Not OK. This information can also be used by fraudsters to access your accounts as family names and dates of birth are often used by people to remember their passwords.

9. **Names of family pets**

Not OK. This information can also be used by fraudsters to access your accounts as names of family pets are often used by people to remember their passwords.

10. **Schools attended**

Not OK. This information can also be used by fraudsters to access your accounts as schools are often used as a security question to verify your identity.

It is always worth thinking hard about what information you put about yourself into the public domain. Think about:

- Who might use it in the future
- How might they use it in the future
- Once it is there, it is almost certainly always there.

Use the privacy settings to block your personal information from all but those you are comfortable seeing it! Otherwise, your personal information is there for people like Malcolm to use; and that might result in a crime being committed against you.

But what about the telephone calls you receive at home and the many mail-shots? They might be a nuisance, but from time to time people offer you products and services that you are actually interested in! Imagine the scene – you have a glass of wine in your hand, you have your feet up and are relaxing after a stressful day at work. The telephone rings ...

**Extract from telephone call**

"We are delighted to inform you that you have won the first prize in our prize draw, a marvellous Lexus GS SE 5 seater saloon worth £100,000. All you have to do to claim your prize is to call 0901 222 1234 within the next twenty four hours and to have your credit card details to hand to pay for delivery right to your door. To be eligible for this prize you agree without reservation for your name and address to be published."

1. **Could this be you? You remember entering a prize draw and you are delighted to have won**

**Yes**

Tread carefully. You may really have won something but follow the mantra 'if it seems too good to be true, it probably is'. Avoid giving your credit card details. If you think you really have won, find some other way to pay that limits your risk and protects you from possible future fraud.

**No**
Avoid following up. This is almost certainly a hoax. The trickster wants your credit card details and your full address. Once he has them, he'll spend against your account.

2. **You think the cost of delivery is a small price to pay for a £100,000 car. It seems reasonable!**

**Yes**
If it sounds too good to be true, it probably is. Ask yourself why anyone would give you a £100,000 car for nothing.

**No**
If they are going to give you a £100,000 car for nothing, you might at least think they would throw in the cost of delivery!

3. **Could this be you? You balk at having to dial a premium rate 'phone number and bin the letter.**

**Yes/No**
At best, scams of this type are about nothing other than clocking up premium rate telephone revenues. Better to be safe than sorry! Don't take up the offer!

4. **You decide to call the number. If the cost of delivery is over £100 you'll be covered by the credit card company if anything goes wrong.**

**Yes/No**
No credit card company will cover you for any losses. You would willingly be giving your credit card details to what is almost certainly a scam and you cannot expect the credit card company to protect you.

5. **You call the number and provide your credit card details.**

**Yes**
Once you give away the 16 digit number from the front of the card, the issue and expiry date and the 3 digit security number from the back of the card, you have authorised payment. What's more, you have given the person at the other end of the line everything they need to make their own purchases using your card details. If you follow this course, you can almost certainly rely on two things: you'll never take delivery of your new Lexus car; and your next credit card statement will be a shock!

**No**
Your personal information has value to others. Always protect it!

6. **Could this be you? Your name and address in exchange for a £100,000 free car? No contest!**

**Yes/No**

Until now, the caller only has your ‘phone number. If the caller has used a ‘sequential dialler’, i.e. the caller dials the next number in a sequence, of numbers, s/he has no idea of your name, or your address, which is why often these calls begin, ‘are you the owner / occupier?’

People who call you ‘cold’ are often fishing for more information about you, either to sell you something you don’t want or need, or to obtain information about you that they can later use, sometimes perfectly legitimately, but sometimes, possibly not. If what they are offering you seem too good to be true, it probably is! It could be that Emma fell victim to fraud and identity theft precisely because she gave away personal information to someone calling her cold at home. Remember! Your personal information has value. Guard it well! And guard the personal information of your colleagues and customers as you would expect your own to be guarded. In your personal life, you would not want to fall victim to identity theft or financial crime. And at work, you would not want to be the person who inadvertently allowed personal information to fall into the hands of fraudster s who, through your action, gave them enough to prey on their victims!

## 4. A customer database is accessed

Your investigation into Emma's situation whereby she has fallen victim to fraud and identity theft has led you to Anil. Anil works in the Operational Risk department of the share registrars who administer the shares Emma recently sold. From Anil you learn that a customer database which includes Emma's personal information and details of her share holdings has been recently accessed by a member of staff who, records show, had already left the company. Now read Anil's statement made at the time:

"As with most large corporates, because every user who logs on to our systems has a user name and password, and because these are recorded at date and time of logging on, it is a simple matter for us here in Operational Risk, to get reports that show who logging on to which company systems, what they are doing when they have access, when they are doing it and when they are logging off. Of course, not every user has access to sensitive information such as customer databases. But we keep very tight control over which employees have access to what. If, for example, an employee moves departments, we review what systems they need access to in their new job, ensure they have access to those systems, and remove their rights to access the systems they no longer need to use. Similarly, if someone leaves the company, we remove all their access rights immediately we have confirmation of their departure. When we pulled off a report just a few weeks ago, I couldn't help noticing that Malcolm King had recently gained access to the customer database. Now I knew Malcolm a little, and although I hadn't seen him for a while, I was sure I had heard he had left the company, so I began to be suspicious. I decided to investigate a little further."

It quickly became apparent that Malcolm had not only accessed the customer database but had copied it to his office PC, which means that somehow, after he had already left the company, he had gained access to the office. And it didn't end there. Once the database was copied to his office PC, he opened Outlook and composed a new message:

From: malcolmk@sharereguk.com
To: malcolm.king@imail.com
Subject: Information
File: attachment: db.mdb
See attached.

When I checked Malcolm's personnel record, I noticed we had a personal email address on file for him. It was malcolm.king@imail.com. Clearly, he had sent the email and the entire customer database to his personal email account which is a serious breach of security and if he had still been employed by us, would have cost him his job. Malcolm had tried to cover his tracks by deleting the email from his Outlook account, but what he would not have realised was that the email was still held on the company's server and I was able to retrieve it from their with the data and time stamp. I began to think of the risks associated with this customer database having left the security of the company's server.

The risks Anil identified are listed below. Now rank these risks in order of importance, '1' being most important, '4' being least importance.

1. Malcolm wants to use the database himself. He plans to set up his own business and sell his services to his former company's customers.

Malcolm has stolen company information. Contacting these customers would put him in breach of the Data Protection Act since he has not first obtained their permission for him to

contact them. In any case, his company might well want to prosecute him for having stolen the data.

2. Malcolm wants to use the database himself. He plans to contact the customers on the database claiming still to be working for his former employer. He will sell his services and have customers pay their fees into a bank account set up to receive their payments.

Malcolm has stolen company information and he is committing a fraudulent act by falsely telling customers that he still works for his former employer, regardless of whether or not he persuades them to buy his services. His actions leave him liable to prosecution.

3. Malcolm, having been approached in the pub close to where he worked, sees a chance to make some money by selling on the customer database. He hasn't asked too many questions about what will be done with it after he has passed it on.

Criminals target pubs near call centres and major office blocks. Malcolm has stolen company information and in selling it on to potential criminals is liable to prosecution.

4. Malcolm's PC has anti-virus software and a firewall, but his subscription for updates has lapsed. He has a wireless broadband connection but he's never really worried about what if any security he has.

Malcolm has stolen company property. Even if he does nothing with the database, he has left all the customers whose details are on the database vulnerable to risk because his personal PC is not secure. Cyber-criminals could easily gain access to the database through his unsecured wireless broadband connection and then target their victims.

You now know that the customer database containing Emma's contact details has been compromised, and that Malcolm has copied it and sent it to his own personal PC at home some time after he had left his employer. The fact that Malcolm managed to access the database and his Outlook account after he had left means that the advice from his line manager that he was leaving the company was either never sent to Operational Risk, or it was never received. You have identified that Tony was Malcolm's line manager. Tony has only been with the company for six months and it is quite possible that Operational Risk not receiving advice of Malcolm's departure was an oversight on Tony's part. Nevertheless, you decide to investigate further. You have four different avenues to investigate. You must investigate them all, but it is up to you which order you choose to investigate them.

1. **CV**

When Tony applied for his job, he submitted his curriculum vitae (CV). You now have the chance to view his CV. When recruiters look at CVs they like to be confident that what is being stated on a CV is true, and they check very carefully, including following up on any referees provided.

**References:**
An extract from a reference from ShareDeal Services Ltd:

Dear Sir, Reference for Tony Hawkens:
Tony was employed by us as Customer Experience Team Leader between 6 August 2007 and 4 July 2008. He was a reliable and punctual individual who always delivered work to the required standard. We would be happy to employ him again if a suitable opportunity arose.
Yours sincerely,

A Hamilton

**Previous Jobs :**
Note from Anil: 'Check whether anyone has checked what Tony was doing between 4 July 2008 and 10 November 2008?' 'Seems not to stay in any job longer than a year'

**Qualifications:**
Extract from letter from University of West Sussex stating that they have no record of Tony Hawkens as a student at the university between 1995 and 1998 let alone anyone of that name having graduated.

Extract from letter from University of East Sussex stating that Tony Hawkens was a student at the university between 1994 and 1997 and that he was awarded a BA (Hons) 2(ii) in 1997.

**Schooling:**
Illustrations of certificates supporting these grades.

**Membership of professional body:**
Extract from letter from the National Institute of Marketing.

Dear Sir
Ref: Mr Tony Hawkens
We are able to confirm that Mr Hawkens was a member of this Institute until July 2008 when his membership lapsed. We did try to contact him to invite him to renew his subscription but our communications were un-answered.

So there are some discrepancies on Tony's CV. He appears to have falsified some of his qualifications, inflated a recent job title and claimed to be a member of a professional institution from which his membership has in fact lapsed. His employment record shows he never stays in any job for more than a few months. There is also a gap in his employment history. What was he doing between July and November 2008? If these are, indeed, false claims, Tony is guilty of fraud because he has dishonestly made a false representation.

## 2. Absence record

Like Anil, you now have a record of Tony's absences since he joined the company. Within two weeks of joining, Tony had a day off work to attend a follow-up visit to a cardiologist at the local hospital. Three months later, he is shown as having been off sick on a Monday, Tuesday and Wednesday suffering acute angina pains. Two months after that, Tony saw the cardiologist again for a further follow-up and review of his medication. Like Anil, you might naturally feel sympathetic. You had no idea that Tony had been ill. But you nevertheless check further and find that Tony joined the company having completed a medical questionnaire which he had completed but which makes no reference to any pre-existing medical conditions. Since only a random sample of new starters are required to attend medical examinations by independent GPs, Tony was never examined by a doctor prior to commencing work.

## 3. Company benefits

Like all employees at his level, Tony has the benefit of life assurance provided as a benefit by the company. You realise that Tony claims on his application for life assurance that he has no pre-existing medical conditions.

## 4. Expense claims

Tony's recent expense claims now come to light. According to his expense claims, you discover that he claimed a mileage allowance for travelling by car from London to Manchester three months ago. The amount of the claim was relatively small - just under £160. But the date the journey took place was during his apparent three day absence off sick. He may have made an error inserting the wrong date on his expense claim form. But then you notice in the file that Anil has left a copy of a claim made by Malcolm before he left the company. Anil realised that as a manager, Tony has the authority to sign off the expense claims of the members of his team. The claim is for just under £1000 and appears to be payment of a London restaurant bill for a team celebratory dinner hosted by Tony. You uncover notes of an interview Anil had with Tony. Tony appears to have told Anil that the team celebration followed the winning of a huge contract, that he would have paid for the meal himself but his own line manager was off on long term sick leave and it was just simpler for Malcolm to pick up the bill leaving Tony to sign it off.

Tony appears to have committed a number of frauds: He has dishonestly made false representations on his CV in applying for his current job; It looks as if he has dishonestly made false representations on his absence record; He appears to have failed to disclose pre-existing medical conditions on his application for life insurance; and He appears to have committed a fraud by abusing his position in getting Malcolm to pay the restaurant bill and then signing it off himself. Now find out what Tony had to say when he was finally confronted.

"All the claims I made are true. My CV correctly states I am a graduate of the University of West Sussex. The letter you have from them clearly states that they do not know anyone by the name of Tony Hawkens. They wouldn't. Tony is an abbreviation. The name they will have on file for me is Anthony. I can't comment on any Tony Hawkens who may have attended the University of East Sussex. That's for the university to comment on. I do have angina and I failed to disclose it. I'm sorry for that. But that's my only crime. The gaps in my CV correspond with the time I was caring for my sick mother at her home. I did travel to Manchester, but I must have made a mistake on the expense claim. I went to see a customer and you can check the date with the customer. The date of the meeting is also logged on my Outlook calendar. As for Malcolm, I made a mistake. The poor guy was made redundant. He's not only lost his job but he's going through an acrimonious divorce and his wife won't let him see the kids. I discovered he had left a photo of his kids on his desk along with some other personal possessions and I foolishly gave him the door entry code so he could gain access to the office and collect his belongings. But that's all I did. I haven't stolen anything. I haven't benefited from anything that I've done, there have been no victims. I've done my job and no-one has complained ...."

What does and does not constitute fraud is defined by the Fraud Act 2006. Being convicted of fraud can carry penalties of up to 10 years in prison. As you can see, fraudsters who dishonestly make false representations can be found guilty on the basis of the conduct regardless of whether or not anyone has been deceived. With this kind of fraud, there need, therefore, be no victims. But we nevertheless must always be on our guard - people who falsely obtain our personal information can take money from our bank accounts, spend money on our credit cards, cash in our insurance policies, and in extreme circumstances, as with Emma, hijack our own identities, including our passports and driving licenses, key documents which prove who we are. Fraudsters can harm us as individuals and they can harm our businesses too. According to the National Fraud Authority, losses resulting through fraud cost the UK £30 billion in just one year, the equivalent of £621 per adult. We all have a role to play in defending ourselves, our customers and our businesses from it. Being alert as

we go about our day to day business is a powerful weapon in the arsenal we need to stem the tide of fraud.

## 5. Responding to official requests for information

As you delve further into the investigation into Emma's financial losses as a victim of fraud, you learn that she is a fairly frequent visitor to her online bank account. She is particularly careful when accessing her account from her home PC as she is aware of the dangers of cyber-crime. She has anti-virus and firewall software and she frequently changes the password Emma routinely receives email communications from her on-line bank. Check out one she received recently.

Dear Ms Mullen
We have been working hard to refresh our online internet banking service. You have been invited to check out the new site before it is launched to the entire customer base. If you visit our site before the end of this month, you could receive a case of six bottles of Bollinger Grande Anée 2000 worth nearly £400. To visit our refreshed online banking service, check your up to date statement and benefit from the most advanced security features online banks provide, visit us at: http://www.phbank.co.uk/default

When Emma clicks the link, she is taken to a website:

Welcome to Internet Banking

You have reached our refreshed online banking website. As a valued customer, you now have the chance to visit the new site yourself. All you need to do is to logon as usual.

Emma enters her details:

Account number: **01324821**
Mother's maiden name: **Peyton**
Password: **f001pr00F**

As the password is entered, the screen changes to the 'home' screen of the bank:

Thank you.
You are now logged in Emma Mullen
You have reached our refreshed online banking website. The site is currently suspended because we are undertaking some necessary upgrade work. Rest assured, your details have been logged so that you have the chance to receive your free case of champagne. We will contact you again shortly by email to confirm your win. In the meantime, to maintain security, when leaving this site, please remember to logoff properly.
Logoff

Bill is an IT professional. He is fascinated by how systems work. 'Breaking' systems to see how they work and then putting them back together is a passion for him. One day, as he explored the highly innovative website of a well-known online bank, he had the idea of setting up a 'cloned' site, that is, a site that he would design to look almost exactly like the site of this bank. Having created his cloned site, Bill set about inviting people to visit it. He sent out emails in the style of the online bank, he had cloned, inviting recipients to follow the links to his cloned website. One of these emails was sent to Emma. See what happened when Emma logged into the cloned site:

Welcome to Internet Banking
You have reached our refreshed online banking website. As a valued customer, you now have the chance to logon to your account, see how the new site works for yourself and

answer a simple customer survey to provide us with feedback. All you need to do is to logon as usual.

Emma enters her details:
Account number: **01324821**
Mother's maiden name: **Peyton**
Password: **f001pr00F**

Through an elaborate deception known as 'phishing', Bill now has Emma's account number, her mother's maiden name and her account password, everything he needs to access her real bank account and to empty money from it. Regardless of whether or not he takes money from her bank account, he has already committed a fraud by misrepresenting his 'cloned' site as the site of a major UK retail bank. Even if Emma and the other recipients of Bill's email do not log on to his cloned site and part with their logon details and passwords, he is still, in the eyes of the law, been guilty of fraud by false representation. Nobody needs to have been misled into ***believing*** his cloned site was that of the bank for him to be guilty of fraud. Equally, nobody has to lose anything by logging on to his site for him to be found guilty of fraud. This is because the law says it is enough for Bill to have falsely represented his site as the site of the bank. Bill may just have been experimenting when he established his cloned site. But he could just as easily steal money from all the accounts for which he has gathered logons and passwords. Or indeed, he could sell the personal information he has gleaned from his targets' logons and passwords to criminals who then use it to empty their victims' accounts.

If you receive an email at home or at work, never click directly on links provided in the email. The links may look harmless, but you can just as easily be directed to a fake site from where your personal details will be captured. People like Bill who construct fake sites are just as easily able to infect your PC with a 'trojan horse', (a virus that enables Bill, and people like him, to record your keystroke you tap on your computer keyboard, and so to record your logon and password details). And remember: you can always recognise a secure website if the address begins https:// and if there is a picture of a padlock to the right of the address bar.

## 6. Like a bloodhound

How would you know whether someone was committing some kind of fraud? Some kind of fraud against the company? Some kind of fraud against a colleague? Some kind of fraud against customers? What, if anything would make you suspicious as you go about your daily business, whether in the office at work, or in your private life? The better idea we have of what to look out for, the better able we are to protect ourselves against criminal activity. Often, sudden changes in a person's behaviour or lifestyle can be an indicator; a person who never had much money before and suddenly seems to be spending vast sums without any obvious means of having acquired it; a person who suddenly becomes secretive where previously they were talkative; a person who is never away from her desk or never takes holiday. Of course, there may be any number of legitimate explanations for sudden changes in behaviour; their committing some fraud may be a possibility, or not.

Consider the following scenarios. For each one, decide whether you are suspicious of the character being described or whether in your opinion, they are quite trustworthy. As you make your decision, think about how and why you have reached your conclusion.

1. **Find out about Gloria**

As you have been investigating how Emma may have fallen victim to financial crime and identity theft, your attention has been drawn to Gloria. Gloria is a new employee to the company. She seems to be frequently away from her desk. Every so often, very quietly, she stands up, collects her bag from the floor along with her mobile 'phone and disappears from her department. One day, as you walk past a meeting room, you see her through the window, speaking into her phone. She seems distressed. You go back to your desk, close to where she sits and she returns to her desk shortly after. Neither of you makes any mention of her telephone calls or her distress. Some time later, Gloria leaves her seat, collects her bag and mobile and you decide, this time, to follow her. She stops at the meeting room, pushes the door open, goes in, closes the door behind her and immediately makes a call. This behaviour continues over several days. You know Gloria has access to customers' personal information including bank details. What is she up to? Who is she talking to? What is she planning? Are you: Suspicious of Gloria / Not suspicious of Gloria?

**Suspicious:**
You've no reason to be suspicious. Gloria has a sick mother about whom she is worried and to whom she has to make frequent calls home. This is a private matter and she prefers not to make the calls from an open plan office. Nevertheless, you know Gloria is grateful that you approached her. As a new employee, she did feel that no-one was taking any interest in her.

**Not suspicious:**
Gloria is new. She handles confidential personal information including bank details of customers. She is frequently away from her desk making private calls and often appears distressed. On the one hand, you have a duty to protect your customers and if there is a hint that Gloria might be passing on confidential information about customers, this should be pursued. But equally, if there is something wrong, someone really should approach Gloria and find out what it is. One way or another, you or Gloria's manager, need to find out more.

2. **Find out about Bill**

As you have been investigating how Emma may have fallen victim to financial crime and identity theft, your attention has been drawn to Bill. You have recently taken over as Bill's line manager and you are responsible for signing off his monthly expense claims. You notice

that his expense claims for travel and taxi fares appear to be much higher than the other members of your team who travel as much if not more than Bill, and Bill has had a number of days absence due to sickness over the last month. Bill seems to have receipts for most of his train and taxi fares, but when you challenge him, about a costly inter-city fare, he claims that the ticket office was shut, that he paid his fare on the train and the train manager's ticket machine would not print a receipt. He paid in cash so has no credit card receipt. His mileage claims appear also to be excessive, as you have checked some of his journeys on the internet. During a recent evening out with the team, you learn from colleagues that it is only in the last six months that Bill has been buying rounds of drinks. Previously, he would join them, but before it was his round, he would excuse himself and leave. His new car was very much admired by the team as he drove away that night. Are you suspicious of Bill / Not suspicious of Bill?

**Suspicious:**
Bill's behaviour seems to have changed in recent months. From being someone who would socialise with colleagues but disappear before it was time for him to buy rounds of drinks, he now seems have more cash. He also has a brand new car. Sudden changes in behaviour can be a sign that something fraudulent is taking place. Unfortunately, Bill is unable to produce receipts for all his journeys and you discover that some of his expense claims relate to journeys he claims to have made on days he had telephoned in sick. You have good grounds for being suspicious of Bill and this should be followed up. Cheating on expenses is regarded as fraud.

**Not suspicious:**
If Bill has made a mistake in his expense claim, this needs to be identified quickly. But there is not only his inter-city train fare to consider, but also his mileage claims. The fact that his claims are higher than those of his colleagues and that he suddenly seems to have come into money – sufficient to begin buying rounds of drinks and a new car also makes his actions suspicious. Cheating on expenses is regarded as fraud and you should follow this up.

3. **Find out about Trevor**

Trevor is responsible for making ad hoc payments on behalf of the company to suppliers by cheque. These are typically relatively small sums of money; up to £100 per cheque and are issued only when a proper invoice is supplied. Unusually, Trevor was taken ill over the weekend. No-one in the office can ever remember Trevor taking time off work before for illness. Often, he doesn't even use his full holiday entitlement in a year. But now a cheque needs to be paid, Trevor's desk drawer is locked and the cheque book is inaccessible. Fortunately, Trevor is not the only authorised signatory. You may sign cheques too. You approach Facilities Management, obtain a duplicate key and take the cheque book from Trevor's drawer. You write out the cheque, hand it over to the supplier, file the invoice and are about to replace the cheque book in Trevor's drawer when you notice there are five missing cheques from the book. Trevor is usually very efficient and writes details of the payee and the amount paid on the stubs. However, the stubs to which these missing cheques relate are blank. Are you suspicious of Trevor / Not suspicious of Trevor?

**Suspicious:**
Trevor may be very efficient, but who checks the bank statements? Now is the time to do a thorough check. Have these missing cheques been issued? Have they appeared on any recent bank statements? Have they been paid to legitimate companies? How much were they for? Trevor is never off sick and rarely takes all his holiday. You would have good grounds for being suspicious about Trevor. Fraudsters who defraud their own company often stay close to their desks for fear of what others might find when they are away!

**Not suspicious:**
There may well be a perfectly good explanation for the missing cheques. But Trevor is never off sick and rarely takes all his holiday. Fraudsters who defraud their own company often stay close to their desks for fear of what others might find when they are away. It can take many months for this type of fraud to be detected unless managers are careful to check bank statements regularly and to monitor what cheques are being paid. This is the first step. Asking Trevor to explain the missing cheques is the second.

4. **Find out about Harry**

Harry works in purchasing. He is authorised to sign and place orders with suppliers up to a value of £1000. Any orders over and above this amount must be signed off by a senior manager. You have carried out an audit into the work of the purchasing department and have found eight separate orders, all placed with a supplier that has never done business with you before and all placed over the course of a week. Each order is for £995 and each has been signed by Harry. Are you suspicious of Harry / Not suspicious of Harry?

**Suspicious:**
The placing of eight orders, all to a brand new supplier with whom you have never before done business, and all for under £1000 so not requiring the signature of a senior manager sounds suspicious. Check to see whether any quotes were received from the supplier in writing. Check whether anyone else was asked to quote. Investigate the supplier to whom the order was issued. Is it a legitimate company? Does Harry have any other connection to this company, (e.g. who are its directors? Members of his family)? Authorisation limits are there to protect individuals and companies from the risk of fraud. Finding ways around them put individuals and companies at risk.

**Not suspicious:**
Whether or not Harry committed a fraud remains to be seen. But either Harry is finding ways around the laid down policies to place orders significantly above his authorisation limits, (in which case this may be a disciplinary offence), or he may be colluding with the supplier.

5. **Find out about John**

You were accompanying John on a business trip abroad. The night before the departure he called you to say that his passport had expired, yet the following day, he turned up at the airport with a passport which check-in and immigration appeared to think was valid. You know John is an identical twin. Are you suspicious of John/ Not suspicious of John?

**Suspicious:**
Obtaining a replacement passport overnight is impossible! If John has used his brother's passport, this is fraud by dishonestly making a false representation. The fact that there is no victim does not make John any the less guilty.

**Not suspicious:**
Obtaining a replacement passport overnight is impossible! If John has used his brother's passport, this is fraud by dishonestly making a false representation. The fact that there is no victim does not make John any the less guilty.

6. **Find out about Simon**

You work for an insurance company in their motor insurance section. You take a call from Mr Johnson. He provides you with his policy number and asks to add his son, Simon, who has just past his driving test at the age of 17, to his policy. You ask Mr Johnson some security questions, starting with his date of birth. When he first gives his date of birth, you realise that Mr Johnson himself would only be 17 years old. When he realises his error, Mr Johnson

provides his correct date of birth. You add Simon to Mr Johnson's motor insurance with immediate effect. Are you suspicious of Mr Johnson / Not suspicious of Mr Johnson?

**Suspicious:**
You have good grounds to be suspicious. Of all the things people do not get wrong, it is their date of birth! It sounds like Simon is making the call himself. He cannot afford insurance of his own and he thinks if he quietly adds himself to his father's policy, his father will never know. Simon is acting fraudulently.

**Not suspicious:**
You should be! Of all the things people do not get wrong, it is their date of birth! It sounds like Simon is making the call himself. He cannot afford insurance of his own and he thinks if he quietly adds himself to his father's policy, his father will never know. Simon is acting fraudulently.

## 7. The mind of a fraudster

Be honest! When you think of me, which isn't very often, you think of me as a man wearing a black and white striped sweat-shirt, a balaclava covering my face, a bag hung over my shoulder bearing the word 'swag'! Well I'm happy to go along with that image. After all, if that was a real fraudster, you'd spot me in the street, no problem! And while you're looking for him, you're not looking for me. Because I'm much too clever for you to recognise me.

So who am I? A fraudster? Perish the thought! Not me! No! I'm a collector! I collect things. Mostly, they're things you wouldn't think twice about. Things I pick up as I walk down the street. Things I pick up as I sit listening to peoples' conversations in coffee shops, pubs, bars or railway stations. Things I pick up when I'm travelling on trains or when I'm pretending to be reading the newspaper in hotel lobby and reception areas. Things I pick up when I'm waiting in airport lounges or standing outside the office blocks of large corporates, smoking my cigarette along with the rest of the smokers.

So what exactly do I collect? What is it that I pick up? Well to be honest, anything you throw away or leave behind! A scrap of paper. A jotter. A letter from your bank, or building society, just left on the table as you bend down to reach into your bag. A chance remark on the 'phone is good. Only the other day, a man in a coffee shop was enquiring about the value of his pension fund. Of course, I could only hear his end of the conversation. But that's all I needed. 'Yes,' he said. 'Hendy. Charles Hendy' Pause. 'AB 10 41 76 G' Another pause. '8.2.52' As I peered at the letter on the table in front of him from his pension provider, I had all I needed to empty his pension fund. Easy!

Then there are the mobile phones and smart-phones. You'd be surprised how many people leave these lying around in pubs, or on seats on trains. Of course, it's not the free phone calls that make them attractive. It's the fact that so many of them contain their owner's life story! I have the owners' addresses and contact details. I know from their calendars when they're away on holiday. I have their complete contacts lists. The best ones even tell me their logons and passwords to bank accounts, building societies, shopping accounts. People have so many of these to remember that they record them somewhere – and what better place than their mobile 'phones? After all they carry their mobiles with them wherever they go. That is, unless they've fallen into my hands! PIN numbers? Now be honest! How many people do you see entering a PIN number to access their mobile 'phones?! And even if they do report their loss, there's usually time enough for me to obtain something of value.

And laptops! Magnificent when one of those falls into my lap. Still so many of them around that aren't encrypted. Windows password? Easily cracked! Last week? On the train on the way up to Cheltenham? Yes! That was me! Why would I have your laptop now? I took what I needed from it immediately then discarded it not a mile from the station. But I do have your bank account details, your mortgage details, your pension and insurance arrangements, your passwords. You'd even scanned your passport and your driving license just in case you ever lost the originals. How organised you were! Thinking of travelling abroad? I shouldn't any time soon, if I were you! You'll likely be picked up by the police as they mistake you for a member of that gang that robbed the jeweller's shop recently. There's a good trade in real passports! Me? I'm long gone ... and in any case, I'm someone else now!

So now just stop and think for a moment. You may be someone who never checks your bank or credit card statements. You may be someone who never checks your mortgage statements You may be someone who just throws away your annual pension statement without really looking at it because retirement is so far away, isn't it? You may be someone who throws away your utility bills in the waste or recycling bin without first shredding them.

Chances are, then, you won't be noticing when money disappears from your account, when a purchase is made against your credit card. But you will notice when you come to retire and find there's not a penny in your pension fund. But by then it's all too late. Don't think for a moment you're unique. There's millions out there like you. Me? I make a very nice living thank you. From collecting things, you understand. 'Cos the things I collect bring in a tidy fortune. One way and another! And by the way! I wouldn't hurt a fly! So I'm hardly what you'd call a criminal! Not really!