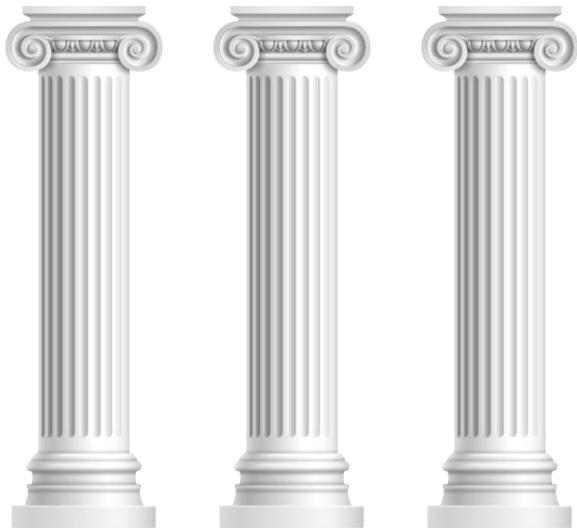




Financial fraud – Common red flags

17 October 2018

The webinar will begin shortly...

Business & Management

20 minute lunch



corporatepartnerships@moneycorp.com



Webinar

Financial fraud Common red flags

Arun Chauhan

Director, Tenet Compliance & Litigation
Director, Fraud Advisory Panel

Wednesday 17 October 2018



**Director
Tenet Compliance &
Litigation**

Purpose of today's webinar

- Provide an overview of financial fraud and the risk from insiders
- Common warning signs
- Three top tips for reducing the risks



Who we are

- We are the UK's leading anti-fraud charity and voice of the counter fraud community.
- We work to improve fraud resilience across the UK and around the world by championing best practice and (where appropriate) law reform.
- Our members cover the full spectrum of counter fraud professionals.

Working together to defeat fraud



Common insider fraud types

- Payroll fraud (expenses/ghost employees)
- Finance function fraud (account manipulation/diversion)
- Recruitment fraud
- Other employee fraud (data/conflicts of interest)
- Supplier fraud (overcharging, manipulation of framework contract)
- Mandate fraud
- Bribery and corruption (procurement/development)



To start – think wider than red flags

- Recent news – insider fraud
- What are we protecting?
- Expectations of our employees' moral compass
- The why?
- Impact of leadership
- Application to risk areas.



Is it possible to profile?

- A man
- Acting alone
- Between the ages of 36 – 45
- In a position classed as ‘senior management’
- Who had been at the victim’s organisation for between 3 – 5yrs
- And who works in the finance department.

Possible indicators of fraud

People

1. Low staff morale
2. High staff turnover
3. Untaken holiday
4. Change in lifestyle/behaviour
5. Long hours
6. Salaries based primarily on performance
7. Conflicts of interest

Transactions

1. Imbalance of work award to a contractor
2. Unusual transactions/reconciliations
3. Excessive payments
4. Duplication of payments
5. Common names or addresses of payees and customers

Possible indicators of fraud

Processes

1. Dominant management
2. Lack of delegation of simple tasks
3. Internal controls overridden without explanation
4. Slow reporting
5. Overly complex systems implemented
6. Lack of internal controls applied without justifiable reason
7. Loss of records
8. Audit findings deemed errors or irregularities
9. Lack of segregation of duties
10. Missing inventory or physical assets

Top three tips for reducing the risks

1. Knowing the greatest risk areas to your business
2. Policies and procedures that people understand, buy into and are consistent with the 'shop floor'
3. Whistleblowing – external and internal opportunities

Free resources at www.fraudadvisorypanel.org

FRAUD FACTS

Issue 3 March 2011 (2nd edition)

Fraud
Advisory
Panel

INFORMATION FOR ORGANISATIONS

Pre-employment screening

It is estimated that almost one in seven CVs contain some form of discrepancy – most commonly dates of employment, academic and professional qualifications and undisclosed directorships*. Pre-employment screening can help your organisation to identify undesirable individuals, who may be dishonest or susceptible to committing fraud, before they join.

What is pre-employment screening?

Pre-employment screening is the process of checking that information provided by a prospective employee – usually in a job application form or CV – is accurate and complete. The results are used to make an informed decision about the suitability of an applicant for a particular vacancy.

To be effective, pre-employment screening should be completed before a prospective employee starts work; otherwise it may be too late.

Why is pre-employment screening important?

Pre-employment screening can provide some assurance that a prospective employee is trustworthy and has the necessary skills and/or experience required to perform the role they have applied for. It can also deter dishonest individuals from applying in the first place.

Pre-employment screening will not completely protect your business against an employee committing fraud once they have started working for you – an individual's personal and/or financial circumstances can change over time – but it can help to reduce the risk of this occurring.

The risks of not screening

Failure to undertake pre-employment screening may expose your organisation to the risks of:

- Abuse of procurement and/or staff expense reimbursement processes.
- Theft of business assets, customer information and/or intellectual property rights.
- Use of your business premises and/or equipment to conduct unauthorised or illegal activities.
- Appointment of individuals not suitably qualified or experienced for the role and/or who are dishonest.

This list is not exhaustive.

Common types of pre-employment fraud†

The applicants:

- Uses a false identity
- Impersonates an innocent party
- Uses a false immigration status
- Provides false education and/or professional qualifications
- Provides false references
- Conceals his or her employment history
- Conceals his or her employment record
- Conceals unspent criminal convictions‡
- Conceals adverse financial and/or credit history.

Key elements

Pre-employment screening can be conducted in-house or outsourced to a specialist pre-employment screening company.

If your business conducts in-house pre-employment screening you should:

- Assign responsibility for it to a specific department.
- Inform all prospective employees that they will be subject to pre-employment screening.
- Ask all prospective employees to sign a full consent form and data protection statement, as well as a declaration to confirm that the information provided on the application form is correct and that they understand any material falsehoods may constitute misconduct and result in the withdrawal of any employment offer.
- Maintain accurate records to demonstrate that appropriate checks have been conducted.
- Monitor relevant legislation and legal requirements (such as checking an applicant's right to work in the UK).
- Establish clear policies to assess the acceptability of pre-employment screening results.

Minimum verification requirements

Employment application forms vary from one organisation to another, but often request information relating to an applicant's:

- Identity (full name and date of birth)
- Residential address
- Educational and/or professional qualifications
- Employment history (including any gaps) and references
- Right to work in the United Kingdom
- Criminal history
- Financial background.

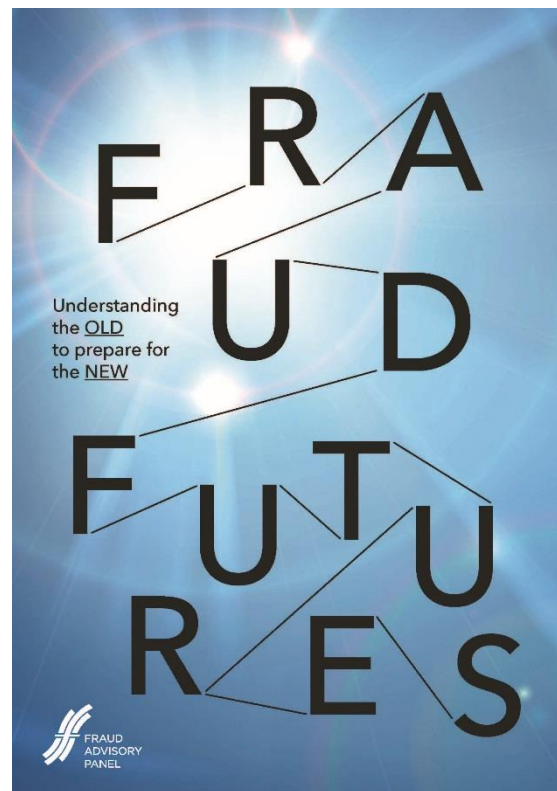
Depending upon the type of vacancy and sector in which your organisation operates, it may be necessary to verify some or all of this information. As a minimum, you should aim to verify the applicant's identity, residential address, eligibility to work in the position applied for and previous employment history.

Government departments and agencies (including the armed forces) must apply the pre-employment screening requirements set out in the HMIC Baseline Personnel Security Standard (BPSS) available from the Cabinet Office website (www.cabinetoffice.gov.uk).

The background checks your organisation conducts should be proportionate to the risks associated with the advertised role. For example, managerial or financial positions may require more extensive screening. Particular care should be taken in screening applicants for positions with access to customer records and/or other confidential information, such as call centre staff.

The Centre for the Protection of National Infrastructure (CPNI) has published useful guidance on pre-employment screening available from the website (www.cpni.gov.uk).

* Researcher (2010). The Researcher Annual Pre-employment Screening Survey 2010.
† Chartered Institute for Personnel Development & CIPD – The UK's Fraud Prevention Service (2007) *Tackling Staff Fraud and Dishonesty: Managing and Mitigating the Risks*



Understanding the OLD to prepare for the NEW

FRAUD
ADVISORY
PANEL



CHARITY COMMISSION
FOR ENGLAND AND WALES



FRAUD
ADVISORY
PANEL

TACKLING CHARITY FRAUD

PREVENTION IS BETTER THAN CURE



SUPPORTED BY



Crowe Clark Whitehill.

A Member of Crowe Horwath International

Webinar

Financial fraud Common red flags

Arun Chauhan

Director, Tenet Compliance & Litigation (www.tenetlaw.co.uk)
Director, Fraud Advisory Panel (www.fraudadvisorypanel.org)

Wednesday 17 October 2018

Business & Management Webinars and events – icaew.com/bamevents

Free 20 minute lunch webinars

Brexit update

23 October 12.30pm

icaew.com/lunchoct2

Bring your own devices policies

6 November 12.30pm

icaew.com/lunchnov2

Stats skills in Excel – waterfall graphs

28 November 12.30pm

icaew.com/lunchnov

Free 60 minute webinars

Team leadership and management

14 November 10:00am

icaew.com/bamnovwebinar

Practical Excel tips

6 December 10:00am

icaew.com/bamdecwebinar

Business tax update

12 December 10:00am

icaew.com/bamdec2webinar

Online e-learning

Leadership in an era of distraction

21/22 November 9.30am

icaew.com/leadership18

Free event

Innovation and business development

13 November 6.00pm

icaew.com/bamnovevent

Business & Management

THANK YOU FOR ATTENDING

Contact the Business & Management Faculty

icaew.com/bam

✉ bam@icaew.com ☎ +44 (0)20 7920 8508

@ICAEW_finman

🖱 icaew.com/joinbam

