

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 applicant:

- 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 conviction(s)
- 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 HMG 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).

* Powerchex (2010) *The Powerchex Annual Pre-employment Screening Survey 2010*.

† Chartered Institute for Personal Development & CIFAS – the UK's Fraud Prevention Service (2007) *Tackling Staff Fraud and Dishonesty: Managing and Mitigating the Risks*.

Who should be screened?

All permanent staff should be subject to pre-employment screening, as well as contractors and temporary staff such as cleaners, security and reception staff. Fraudsters may try to obtain entry to your organisation through temporary or contracting roles where screening may be lax or non-existent.

How to verify information

The process for verifying information does not need to be complicated or expensive. Information can be checked using online sources or by contacting relevant organisations direct.

Identity (full name and date of birth): An original government-issued identity document such as:

- **A current passport:** There are many internet-based passport verification tools available, some of which charge an annual subscription fee. Visit the Public Register of Authentic Identity and Travel Documents Online website for free information on some European countries (www.consilium.europa.eu/prado).
- **Photographic driving licence (including paper counterfoil):** Some of the above verification websites also provide information about driving licences.
- **Birth certificate:** Many include a watermark. It should be accompanied with a marriage certificate for a married female applicant who has changed her name.

Residential address: An online address verification search will return details of companies who can confirm whether an applicant lives at the address provided. Alternatively, you could request a recent and original bank statement or utility bill to verify the address. Address verification can become complicated if the applicant has opted out from displaying his or her details on the electoral register or is not on it.

Education and/or professional qualifications:

Always contact the awarding body directly to verify the degree or qualification, dates of attendance and grades received.

Employment history: Look online to see whether the organisation exists and contact it direct to confirm the applicant's length of service and duties. Many organisations will ask to see the applicant's signed consent form prior to releasing

any information. A P45 or P60 could be requested for further confirmation. Request references for previous employers and check employment gaps greater than three months.

Right to work in the United Kingdom:

Visit the UK Border Agency's website (www.bia.homeoffice.gov.uk) for information on how to check that a prospective employee is entitled to work in the United Kingdom. See the dedicated section for employers and sponsors on preventing illegal working.

Criminal history: Can be obtained from the Criminal Records Bureau, Disclosure Scotland or Access Northern Ireland (Access NI). There are different levels of disclosure which are dependent upon the role being applied for and the position of trust it entails.

Other searches: You may also wish to consider undertaking money laundering, credit searches, disqualified directors and/or individual insolvency searches, depending upon the type of vacancy being filled.

Taking action

A prospective employee who submits a false employment application form may have committed offences under the Fraud Act 2006, as well as a number of other relevant Acts.

If you discover that a prospective employee has provided a serious material falsehood on his or her application form for employment with your organisation, you should:

1. Withdraw any offer of employment that has been made.
2. Report the matter to the appropriate authorities (such as the Police, UK Border Agency, etc).
3. Notify any recruitment agency involved that a fraudulent employment application form has been submitted.
4. Record the fraud on the CIFAS Staff Fraud Database (if you are a member).

Ongoing reviews

Finally, your organisation may wish to consider conducting periodic checks on employees being promoted, as well as in high risk positions, to ensure they remain fit and proper for the role performed.

Important note: money laundering regulations

If your business is within the scope of the Money Laundering Regulations, then you are likely to have a duty to make a Suspicious Activity Report to the Serious Organised Crime Agency (SOCA) where you know or suspect that an individual has taken up employment with your firm, or anyone else, on the basis of a criminally fraudulent CV. This is on the basis that any salary paid will constitute the proceeds of crime.

Further information

Access Northern Ireland
www.accessni.gov.uk

Cabinet Office
www.cabinetoffice.gov.uk

Centre for the Protection of National Infrastructure
www.cpni.gov.uk

Chartered Institute of Personnel and Development
www.cipd.co.uk

CIFAS – the UK's Fraud Prevention Service
www.cifas.org.uk

Criminal Records Bureau
www.crb.homeoffice.gov.uk

Disclosure Scotland
www.disclosurescotland.co.uk

Fraud Advisory Panel
www.fraudadvisorypanel.org

The Insolvency Service
www.insolvency.gov.uk

Public Register of Authentic Identity and Travel Documents Online
www.consilium.europa.eu/prado

Serious Organised Crime Agency
www.soca.gov.uk

UK Border Agency
www.bia.homeoffice.gov.uk

*The Fraud Advisory Panel gratefully acknowledges the contribution of **Gaby Devereux** (CIFAS – the UK's Fraud Prevention Service), **Richard Evans** (AXA Life), and **Carl Watson** (Chantrey Vellacott DFK) in the preparation of this Fraud Fact Sheet.*

Distributed by

Fraud Advisory Panel, Chartered Accountants' Hall, PO Box 433, Moorgate Place, London, EC2P 2BJ.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Registered Charity No. 1108863

Disclaimer

Dissemination of the contents of this Fraud Fact Sheet is encouraged. Please give full acknowledgement of the source when reproducing extracts in other published works. Whilst every effort has been made in the construction of this Fraud Fact Sheet, compliance with it does not guarantee that you and/or your business will not be a victim of fraud or criminality aimed against you and/or your business. The Fraud Advisory Panel and the contributors to this Fraud Fact Sheet accept no responsibility for any action taken by parties as a result of any view expressed herein. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them or their business.

© Fraud Advisory Panel, 2011