PASA Cybercrime and Fraud Working Group

Produced in partnership with:

Crowe

PASA Experts for Cybercrime & Fraud

Pre-employment vetting

April 2022

Pre-employment vetting

Acknowledgments

PASA is grateful to the authors of the Guidance and members of the PASA Cybercrime and Fraud Working Group (CFWG) and their employers.

Paul Sturgess (Board Sponsor)	**PASA Board Director**
Jim Gee (Chair)	**Crowe UK LLP – PASA Experts for Cybercrime & Fraud**
Andy Cassin	**WTW**
Gillian Baker	**Hyman Robertson LLP**
Justin McLelland	**Stephenson Harwood**
Kate Whitford	**Stephenson Harwood**
Michael Walters	**Invensys Pension Scheme**
Philip Goodchild	**Stephenson Harwood**

1. Introduction

There are many aspects you need to check when making a new hire, and all are important. But we've recently been made aware of fraud undertaken or assisted by employees of administrators, with one such example including people deliberately gaining employment with the specific intention of committing fraud. To counter this, pre-employment checks need to be as effective as possible This Guidance has been developed to support administrators making decisions on the extent of checks required.

This Guidance indicates the types of checks which can be carried out and the information which can be verified, rather than what should be done in every case. Administrators are responsible for ensuring any checks and vetting are:

- proportionate, necessary and relevant to the level of risk associated with the position being recruited
- carried out in accordance with applicable law, including under the UK General Data Protection Regulation and Data Protection Act 2018, the regulatory regime under the Rehabilitation of Offenders Act 1974 and the Equality Act 2010

If you're unsure of what checks you can legally undertake and what information you can legitimately process as part of your verification process, you should obtain expert legal advice. There are also various professional bodies which provide detailed guidelines on pre-employment checking, such as the guidance issued by the Chartered Institute of Personnel and Development (CIPD) (**available online**), which can help you understand what's appropriate and the risks to consider.

2. Deciding what the level of risk is

The level of risk associated with a particular position isn't simply linked to the level of seniority, although this is one factor. It's possible for individuals in relatively junior positions to have access to key parts of a process. For example, information returned by prospective beneficiaries about their identity or bank accounts, or the ability to copy and transfer data – which means there's a higher level of risk.

Administrators should consider risk rating key positions by considering if a dishonest person were to obtain employment in this area, what might they be able to do. You could seek expert assistance if necessary.

3. What information and checks are available?

A lot of information can be lawfully obtained from the public domain. This can be used to verify the information provided by the candidate and to check the suitability of the applicant for a position carrying a higher level of risk. Information isn't always available but can be found in most cases.

Administrators should consider which information would be relevant to verify and which checks would be appropriate and proportionate. They should provide the candidate with relevant information (as required under

data protection law) on the checks being carried out, ensuring compliance with GDPR transparency requirements. A privacy notice for candidates can be used to inform them of the types of information which will be checked, the purpose of processing this data and the legal basis for this processing. Candidates should also be provided with the opportunity to respond to any information sourced online.

While not all the information listed below would be relevant to every candidate, administrators should consider whether verification checks against these information types are applicable. Care should be taken in all cases to ensure any information accessed online, or from other publicly available sources, is accurate and up to date.

The associations of the individual concerned

This includes:

- Employment history
- Any directorships
- Any shareholdings
- Persons with significant control of a company
- Disqualified Directors
- Associations with offshore entities

Residency

- Electoral registration (current and historical)
- Former and current address information
- Telephone landline subscriber at the address
- Insurance paid from the address (motor or household)
- Personal verification

Property

- Ownership information
- Current estimated value
- Charges (debt or mortgage)
- Maps and imagery
- Planning applications

Financial

- County Court Judgments
- Bankruptcy
- Bankruptcy Restriction Orders
- Individual Voluntary Arrangements to make repayments
- Debt Relief Orders

Personal

- Social media profiles and posts (with world-wide geo-location data, where available)
- Website ownership (current and historical)
- Historical website references which are no longer visible online
- Email accounts (verification)
- Mobile telephone (confirmation the number is live, service provider information)
- General media reporting (adverse or otherwise, including court reporting)
- Previous names
- Deceased persons register
- Associations with other subjects and organisations
- Global sanctions and compliance lists
- Politically Exposed Person associations
- Professional registrations and disciplinary action
- Verification of qualifications

4. How to use such information

Not every source of information will be relevant in every situation and each must be checked for its accuracy. However, thoroughly checking the information provided by the job applicant can reveal discrepancies, leading to further checks being necessary. It's also important to compare any information obtained from pre-employment vetting as further discrepancies may be found.

Research undertaken in 2019 by the University of Portsmouth's Centre for Counter Fraud Studies[1] indicated, across one study of 619,000 pre-employment checks, 32% of CVs had material discrepancies. It also showed a significant proportion of those who obtained employment by falsifying their references then went on to undertake other types of fraud within the employer organisation.

5. Conclusion

Given the importance and sensitivity of the work undertaken by administrators, the large payments being made and the overall value of the sums being handled, some are inevitably going to be targeted by fraudsters. This Guidance is intended to outline the pre-employment vetting administrators should consider conducting, in a proportionate and lawful way, to protect them against this problem.

[1] 'The Real Cost of Recruitment Fraud' – Centre for Counter Fraud Studies at University of Portsmouth and Crowe UK LLP - 2019

PASA

assess | aspire | achieve

Get in touch:

info@pasa-uk.com

www.pasa-uk.com

PASA is a Community Interest Company and our full name is Pensions Administration Standards Association CIC. Company number: 6597097