

Watchdog

Pre-Employment Screening 2010

A special edition of The Watchdog – The Journal of The Security Watchdog

EQUALITY ACT 2010 AND PRE-EMPLOYMENT SCREENING

Since the Equality Act 2010 came into force on 1 October 2010, it is no longer lawful for employers to ask job applicants health or disability-related questions prior to making offers of employment, except in limited prescribed circumstances.

The reasoning behind this is to deal with the problems experienced by job applicants with health or disability issues when faced with pre-employment health questionnaires. The aim of the new legislation is therefore to deter employers from using disability or health-related questions to screen out disabled job applicants unfairly.

The law

The Equality Act states that an employer must not ask about an applicant's health either before offering them a job or short-listing them for a job, unless one of the prescribed circumstances set out below applies.

An unsuccessful applicant who has been asked pre-employment health-related questions can bring proceedings against the potential employer if they believe they were not offered a job, or not shortlisted for a job, as a result of their answers to those questions. In this event, the Tribunal will assume the employer has discriminated against the applicant unless the employer can prove that its refusal was non-discriminatory and was not connected to the applicant's answers to the health questions. This is unlikely to be easy for the employer.

Penalties on employers who fail to comply with the new provisions may include, as well as litigation in the Employment Tribunal for discrimination, enforcement action

from the Equality and Human Rights Commission (EHRC). The EHRC has the power to carry out investigations if they believe or it is reported to them that a person has carried out an unlawful act. The EHRC can then recommend necessary actions to avoid the continuation of those acts, for example, an order to stop using pre-employment questionnaires. Investigations also produce draft reports which may be admissible as evidence before a Tribunal.

Prescribed circumstances

As stated above, there are a few prescribed circumstances in which pre-employment health questions can legitimately be asked. They are:

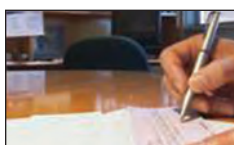
- whether any reasonable adjustments need to be made, either for the job itself or for an assessment in the interview process;
- whether the applicant will be able to fulfill an "intrinsic" function required by the job (e.g. heavy lifting);
- to monitor the diversity of applicants;
- to take positive action to assist a disabled person where that is allowed by other provisions of the Equality Act; and
- if the job requires the applicant to have a particular disability.

If an employer still intends to use pre-employment questionnaires, notwithstanding the new legislation, they must ensure that the reasoning for doing so can fit within one of the

continued on page 2



p5 ICO campaign launch



p7 Identity fraud



p8 Immigration



p10 Media Searches

SECURITY WATCHDOG

from page 1

above exceptions. However, employers should be advised that these exceptions are likely to be interpreted narrowly by the Tribunal and it would be unwise for employers to attempt to rely on these exceptions when continuing to use pre-employment questionnaires without taking prior legal advice.

Referencing

There has been considerable debate within the pre-employment screening industry as to how the Equality Act 2010 will affect the ability for references to request information relating to an individual's time and attendance and the number of days sickness they have taken within the last 12 months based on the restrictions applied by The Act.

Ultimately, The Act clearly focuses on the decision making that has taken place within the recruitment process prior to an offer of employment being made. The majority of pre-employment screening takes place after an offer has been made and the offer is subject to successful completion of pre-employment screening. For this reason the majority of companies still feel comfortable in requesting this information within their references, as any decision that is made based on adverse findings in the area of sickness and absence is the same as before The Act was introduced and is based on policy and risk.

Where the issues may lie is when elements of the pre-employment screening process are initiated prior to the offer stage and the decision as to whether a formal offer is made is subject to the results of referencing. In these scenarios such references should be strictly limited to factual information and omit any questions related to sickness etc.

Summary

It is important that all employers that routinely use pre-employment questionnaires review their practices and consider whether the information that they seek to obtain from those questionnaires is essential to the recruitment process and the particular vacancies in question. A standard practice of issuing questionnaires to all applicants regardless of the position applied for is no longer appropriate.

If employers do believe that health information from applicants is still necessary, employers should comprehensively review their questionnaires and ensure the questions are tailored to ensure they fall within the permitted exceptions. This should be done as soon as possible given that the Equality Act is now in force.

It is also important that employers do not forget their obligations under the Data Protection Act 1998 (DPA), which now align with obligations under the Equality Act. DPA guidance explains that health-related information is "sensitive personal data" under the Act and, if it is relevant to a position, it should be asked for once a decision to appoint has been made, not at the outset of the application process as a matter of course.

This ties in with making conditional offers under the Equality Act, whereby an offer is made subject to receiving satisfactory health responses. As a result, the request for sensitive personal data is made as late as possible and is only requested where necessary.

The purpose of this article is to clarify how the Data Protection Act 1998 (DPA) applies to employment references in relation to the handling by the employer/'data controller' of references written 'in confidence' by referees and subject access rights of candidates/employees.

References written 'in confidence'

Employers are uncertain whether they can release a reference to the person who is the subject of the reference, particularly if the reference has issued by a referee 'in confidence'. Equally they are unsure how the Act applies to these references. The Information Commissioner's Office (ICO) guidance will sometimes appear to counter advice issued by law firms, leaving HR departments nervous that any wrong next steps could lead to possible litigation.

However, the overriding principle of the DPA is that individuals have a right to a copy of the information about them covered by the Act. When an individual asks for a copy of a reference written about them during the pre-employment screening process, many prospective employers refuse to provide it because it was supplied 'in confidence'. This may breach the Act; therefore in cases where the individual asks for a copy, each 'in confidence' reference issued should be carefully considered in a case by case basis before next steps are agreed.

The below FAQs issued by the ICO seek to support a policy for subject access requests:

Does a referee have to give a copy of a reference which they have written?

If an individual asks for a copy of a confidential reference about them written relating to training, employment or providing a service, the referee does not have to provide it because of an exemption in the Act. However, the referee may choose to provide the information. It would seem reasonable to provide a copy if a reference is wholly or largely factual in nature, or if the individual is aware of an appraisal of their work or ability.

Does a new employer have to give a copy of a reference which they have received from a referee?

If a new employer holds the reference in a way that means it is covered by the Act, the employer must consider a request for a copy under the normal rules of access. An individual can have access to information which is about them, but may not necessarily have access to information about other people, including their opinion, provided in confidence.

The references received by a new employer may be marked 'in confidence'. If so, the employer will need to consider whether the information is actually confidential and what express assurances of confidentiality were given to the referee during the referencing exercise. In respect of The Security Watchdog, it is standard practice to assure referees in writing that any references will be treated in confidence during the reference process.

An employer cannot sensibly withhold information which is

‘IN CONFIDENCE’ REFERENCES AND SUBJECT ACCESS RIGHTS

already known to the individual. Factual information such as employment dates and absence records will be known to an individual and should be provided. Information relating to performance may well have been discussed with the employee as part of an appraisal system.

Where it is not clear whether information, including the referee's opinions, is known to the individual, the employer should contact the referee and ask whether they object to this being provided and why.

The employer should weigh the referee's interest in having their comments treated confidentially against the individual's interest in seeing what has been said about them. When considering whether it is reasonable in all the circumstances to comply with a request, the employer should take account of factors such as:

- Any express assurance of confidentiality given to the referee during the referencing exercise.
- Any relevant reasons the referee gives for withholding consent
- The potential or actual effect of the reference on the individual
- The fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
- That good employment practice suggests that an employee should have already been advised of any weaknesses
- Any risk to the referee
- The employer should consider whether it is possible to keep the

identity of the referee secret

In most circumstances, the employer should provide the information in a reference, or at least a substantial part of it, to the person it is about if they ask for it. Even if the referee refuses consent, this will not necessarily justify withholding the information, particularly where this has had a significant impact on the individual, such as preventing them from taking up a provisional job offer.

However, there may be circumstances where it would not be appropriate for an employer to release a reference, such as where there is a realistic threat of violence or intimidation by the individual towards the referee. This is a serious consideration for many employers.

The above relates essentially to employment references. The Security Watchdog undertakes the below list of checks for candidates with their consent. We have noted that it is seldom for any check, other than employment checks, to be labeled with an ‘in strictest confidence’ tag requiring case by case consideration from new employers as to whether this can be copied and issued to the individual, as the data contained within these is, in the main, open source or based on solid fact supported by the protocol that it has been collated with the consent of the individual on behalf of our client in accordance with the DPA. The matrix below is designed to give guidance to clients in this area and support required actions following a subject access request:

LIST OF CHECKS	COMMENT
Identification check	The candidate has provided ID documentation originally and so the results of any ID check can be copied and shared with the individual in a subject request scenario
Eligibility to work in the UK	The candidate has provided eligibility to work documentation originally and so the results of any eligibility to work can be copied and shared with the individual in a subject request scenario
Residency verification (past 3 years)	The candidate has provided residency information and open source databases are used to verify. This information can be copied and shared with an individual in a subject request scenario
Financial Probity check (past 3 years)	The individual has consented to TSW undertaking a financial probity check (consumer database search). This sensitive information is also available to the individual, should they choose to undertake this check on themselves. This information can be copied and shared with an individual in a subject request scenario

FSA Prohibited persons check and individual search	The individual has consented to TSW undertaking an FSA Prohibited persons check (consumer database search). This information is open source and is also available to the individual, should they choose to undertake this check on themselves. This information can be copied and shared with an individual in a subject request scenario
Sanction list check	The Sanction list database comprises factual data from over 150 international open source barred listings. This information can be copied and shared with an individual in a subject request scenario
CV verification	The candidate has provided the CV originally and so the results of CV check can be copied and shared with the individual in a subject request scenario
3, 5, 10 year employment checks	Please apply guidance above on a case by case basis for 'in confidence' references
Highest Educational establishments check	The education checks results are based on facts and can be copied and shared with the individual in a subject request scenario
Professional qualifications or memberships check	The professional qualification checks results are based on facts and can be copied and shared with the individual in a subject request scenario
Directorship check	The directorship check results are based on fact and can be copied and shared with the individual in a subject request scenario
Companies House checks (where appropriate)	The Companies House check results are based on fact. This information is open source and is also available to the individual, should they choose to undertake this check on themselves. This information can be copied and shared with an individual in a subject request scenario
Standard Disclosure Criminality check	The candidate will receive a copy of the Standard Disclosure Certificate as well as the Umbrella Body (TSW)
Basic Disclosure Criminality check	The candidate has consented for TSW to undertake the basic criminality check on behalf of a Client and for the certificate to be sent directly to TSW. TSW has built this clause into the declaration of consent to speed up process. Candidates own their Disclosure Certificate. TSW follows strict protocols in ensuring this sensitive information is stored securely and then destroyed; it seeks confirmation from clients before issuing this data that a secure storage policy is in place. This information can be shared with an individual in a subject request scenario, as the actual certificate belongs to the candidate

Subject Access Rights

Data Protection Good Practice Note Checklist

- Handling requests for personal information (subject access requests)
- Individuals have a right under the Act to make a request in writing for a copy of the information held about them on computer and in some manual filing systems. This is called a subject access request.
- Do you have enough information to be sure of the requester's identity?

- TSW operates a best practice policy by requesting proof of identity from requestors to confirm this.
- Are you going to charge a fee?
TSW consults with clients as to whether this is applicable dependent on the background to the request. A maximum fee to cover administration costs is £10 unless medical or education records are involved. The 40 calendar days to respond will start when the fee has been received.

Prepare the response

A copy of the information should be supplied in a permanent form.



ICO launches campaign to ensure private investigators notify

The Information Commissioner's Office (ICO) is concerned that some private investigators are failing to notify the privacy watchdog that they are handling people's personal information. Many private investigators routinely process personal data such as information about people's private lives, financial data and images.

It is a legal requirement under the Data Protection Act (DPA) for all organisations handling personal information to notify the ICO. Currently only 1,626 private investigators appear on the public register, which the ICO considers to be a relatively small part of the industry. The ICO has written to the Association of British Investigators, World Association of Professional Investigators and the Institute of Professional Investigators urging the industry to take note of their legal responsibilities when handling personal information.

David Smith, Deputy Commissioner at the ICO, said: "We want to work with the industry to ensure all private investigators meet the legal requirement to notify us that they are processing personal information. A targeted approach working with stakeholders and membership bodies has proved highly successful in other sectors. We will be writing to organisations providing them with advice and encouragement to notify. However, if that encouragement is ignored, we will take action against those who flout the law. The message is very clear – notify with the ICO or face regulatory action."

In 2009/10 there was a 15% increase in notifications. The ICO saw a surge in notifications among private doctors and solicitors following targeted campaigns. In the same period the ICO successfully prosecuted seven organisations and individuals for failing to notify. The fee for the majority of organisations remains £35.

Worrying Fraud Trends Revealed!

Fraud continues to demonstrate impact of the recession

The analysis of fraud trends during 2009 by CIFAS - The UK's Fraud Prevention Service - reveals a 9% increase in the overall level of fraud, when compared with the previous year.

THIS RISE HAS BEEN DRIVEN BY SOME PARTICULAR FACTORS, MOST NOTABLY:

- the unwelcome return of identity fraud which has led to a 31% escalation in the numbers of victims of fraud
- a 55% increase in false insurance claims and a change in the nature of them as the effects of the recession intensify
- the relentless rise in facility takeover and misuse of facility frauds.

32% surge in identity fraud

CIFAS commented in October 2009 on the reappearance of identity fraud (the use of a stolen or false identity to obtain goods or services by deception). This increase has continued; up 32% in 2009 from the level recorded in 2008. This rise has a direct link to the recession. Fraudsters have seen the reduction in the overall amount of lending taking place during 2009, discouraging many from attempting to commit application fraud (e.g. the use of lies and forged documents in an attempt to obtain products or services). This has led to a 25% reduction in application fraud but has meant that they have returned to stealing the identities of others in order to gain products and services.

Protective Registration (a service provided by CIFAS to help protect individuals at heightened risk of identity fraud) increased by 241% year on year. This is attributable both to a developing awareness among individuals of the threat of identity fraud and how it is perpetrated, and to the growing use of the service by organisations to protect the identities of those whose details have been put at risk as a result of a data breach.

Over 25,000 more victims in 2009

With over 85,000 victims of impersonation, and 24,000 victims of takeover (whose accounts have been hijacked by fraudsters) recorded in 2009 (increases of 35% and 16% respectively on 2008 and an overall increase in victims of 31%), the very real impact of fraud is underlined. Fraud victims can be preyed upon by organised criminals, faceless fraudsters and sometimes even by those close to them. Victims commonly describe feelings of helplessness, vulnerability and not knowing who to trust. This is in addition to the financial impact and time taken to rectify the damage.

CIFAS Communications Manager, Richard Hurley, comments: "The financial cost of fraud is bad enough, but the emotional and psychological effects for the victim must never be underestimated. Fraudsters are adapting their approach in an attempt to ensure that their profits do not suffer during the recession, with absolutely no thought for the profoundly

damaging impact this has on their victims. The role played by online, organised, criminals trading in people's identity details has been frequently reported in recent years, and it is depressing to think that the numbers of victims of fraud demonstrates just how little these criminals care."

Rise in insurance fraud shows increase in premeditated 'accidents'

While insurance fraud has long been difficult to prove (for instance, adding to claims for stolen cars or laptops other items such as mp3 players, mobile phones, cameras and wallets), the 55% increase in cases filed by CIFAS Members during 2009 reveals a trend towards claimants being even more dishonest. The 55% increase in fraudulent claims is driven more by a surge in claims for staged or completely fictitious events than inflated claims for damage and losses actually incurred.

Facility takeover fraud and misuse of facility continue to be double trouble

Previous figures from CIFAS have confirmed the intensification during the past two years of facility takeover frauds (also known as 'account takeover' where a fraudster hijacks an individual's account in order to 'take over' and control it) and misuse of facility frauds (where the fraudster uses an account, policy or other facility for a fraudulent purpose such as receiving fraudulent payments into a bank account, or evading payments on credit card or loan accounts).

In 2009, facility takeover fraud rose by 16% from 2008. This means an increase of over 250% during the past 24 months. A significant contributory factor to this trend is the prevalence of 'phishing' emails (sent by fraudsters to look as though they come from a bank or credit card company, for example, asking for personal details which are then used to plunder the victim's account).

Similarly, misuse of facility has risen by 28% in 2009 and by 115% during the last two years.

The link between these types of fraud runs deep, with fraudsters frequently using both methods: for example, taking over an account to withdraw funds and then using another account to receive these bogus 'transactions'. Richard Hurley explains: "Whether it is an organised criminal obtaining your account numbers online, or someone in dire financial straits misusing their cheque-book account, the net result is still fraud: fraud that costs businesses, the public sector, and ultimately all of us, millions of pounds each year."

Rise in Identity Fraud: *consequences and prevention*

National Identity Fraud Prevention Week 2010 was held on the 18th of October and the number of reported identity fraud incidents has grown each year.

According to an annual study by the Ponemon Institute the cost of UK data breaches increased by 7% between 2008 and 2009, and has risen by a staggering 36% in the past two years. These alarming figures highlight the need for all corporations to ensure that firm disposal procedures are in place for all documents containing personal or confidential information.

The most notorious data breaches in recent years include the loss of computer discs containing personal data of all families in the UK currently claiming child benefit, and the Information Commissioner stepping in to tell 11 UK banks to stop dumping customers' statements in bins on the pavement outside branches.

These types of data breaches not only have a negative impact on reputation and consumer confidence, but also have serious financial implications. Each individual record lost cost UK organisations an average of £64 in 2009, according to the third annual UK study sponsored by data protection firm, PGP Corporation.

Consumers, too, face hefty financial consequences when

their personal data security is breached, each facing the expensive and time-consuming process of safeguarding or restoring their finances and credit ratings.

The law governing the destruction of confidential information is becoming tougher. Just recently changes to the law have given power to the Information Commissioner's Office (ICO), which can now issue penalty fines of up to £500,000 for breaching the Data Protection Act, meaning businesses should be looking towards the services of a professional information destruction company more often to avoid such incidents.

National Identity Fraud Prevention Week aims to raise awareness and provide individuals and businesses with vital information about how to prevent identity fraud from happening. Some examples of steps that can be made include ensuring all unwanted documents, CDs and DVDs are being properly shredded, wiping clean the information held on old computers before disposing of them and regularly changing network as well as PC passwords.



THE SECURITY WATCHDOG ADVISORY BUREAU

IMMIGRATION WORKSHOP

A half day workshop aimed at HR and Recruitment professionals responsible for Identity and Right to Work checks

The Immigration Workshop, undertaken on clients' premises with a maximum of 10 attendees, will offer instruction on the latest changes in immigration and how to undertake best practice identity and right to work checks.

MODULES COVERED:

- Changes to immigration rules • The responsibility of the employer •
 - Best Practice checks and process • Tools of the trade •
- What to look for • How to maintain records for 'Statutory Excuse' •
 - Useful information/reference sources •

Handouts will be supplied. Courses are priced at £499 +VAT (travelling expenses excluded)

“Very informative and worth its value in gold if your company takes security screening and vetting seriously”

LEANDRO F DE BEER

SECURITY OPERATIONS & TRAINING EXECUTIVE – MUNNELLY SECURITY SERVICES



For further information, or to confirm a booking please contact:

Ewan Tweedie – DIRECTOR
E: ewant@securitywatchdog.org.uk
T: 01420 593832

To obtain further information on The Security Watchdog Screening Bureau services or to receive a pricing proposal please contact Steve O'Neil, Sales Director on +44 (0)1428 728714 or email him at steveo@securitywatchdog.org.uk

To discuss how The Security Watchdog Advisory Bureau could assist your organisation in meeting your various screening and vetting challenges please contact Ewan Tweedie, Associate Director on +44 (0)1428 728735 or email him at ewant@securitywatchdog.org.uk

SECURITY

WATCHDOG

CLIENT TRAINING DAY ANNOUNCED

IMMIGRATION AND ID FRAUD

The Security Watchdog is committed to adding value to our clients and fostering the true spirit of partnership. As such we run training days for our client colleagues on a variety of different aspects of pre-employment screening to enable them to enhance their own knowledge and understanding. This heightened level of awareness across the user group assists in strengthening relationships because both parties have a better understanding of what is required to achieve best practice. Client users also

benefit from being more informed on the subject allowing them to liaise more effectively with their business managers.

The next client training day is dedicated to the prevention of illegal working and the identification of fraudulent documentation. As practitioners who invariably view the original documentation this session will change the individual's mindset when examining identity documents and give them greater confidence in the interpretation of visa documents.

DATE: Tuesday 23rd November 2010

SUBJECT: Prevention of Illegal Working and Identification of Fraudulent Documents

START: 10:00 hours

FINISH: 13:30 hours

ADDRESS: Cross and Pillory House, Cross and Pillory Lane, Alton, Hampshire, GU34 1HL

TSW CLIENT PRICE: FREE

STANDARD DELEGATE PRICE: £150 + VAT

Refreshments and a buffet lunch will be provided on the day

If you are a current client of The Security Watchdog and either yourself or a member of your team would like to attend then please inform your Key Account Manager.

Alternatively you can book a place directly by contacting Ewan Tweedie on +44 (0)1420 593832 or email him at ewant@securitywatchdog.org.uk

MEDIA SEARCHES

Do you know what you are getting?

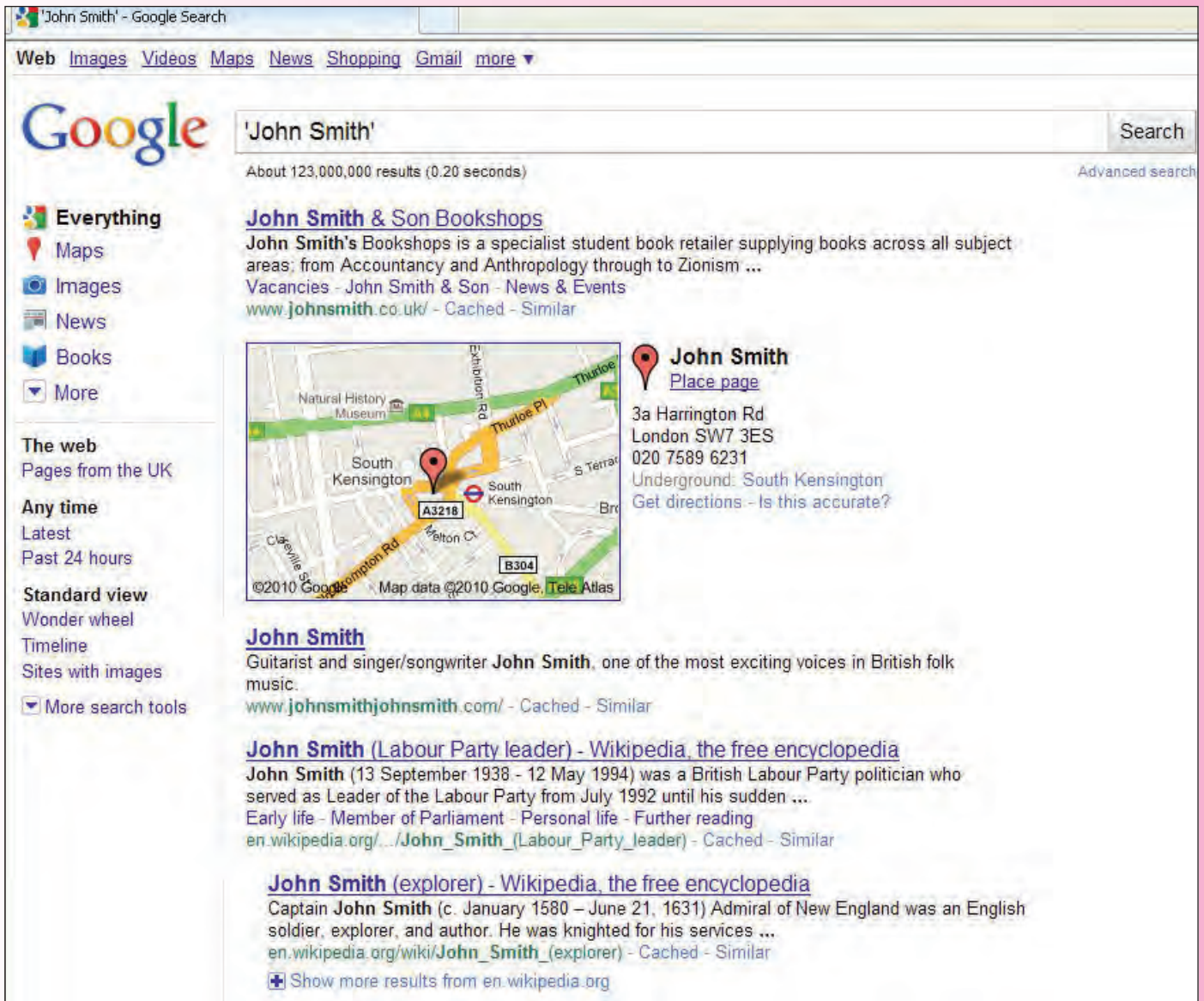
“If in doubt....run a media search!”

Media searches are becoming ever more common place within the realms of pre-employment screening either as a core component of a senior level background check or as a viable workaround to scenarios where data is fundamentally missing or irretrievable.

Whilst a media search can be an invaluable tool to have in the armoury its true value is entirely dependent on the manner in which it is carried out and the tools that are used. The word

‘media’ encompasses a vast range of channels from newspapers, magazines, the internet, journals, television etc. therefore it becomes of critical importance to understand exactly what the word ‘media’ means in terms of a search.

There are many companies that have outsourced their pre-employment screening to a third party provider and routinely conduct media searches as part of their core screening activities. Interestingly, when challenged and asked if they know exactly what they were getting for their media search, only a small



A common name search revealing 123 million ‘hits’.



minority can respond with any certainty. From a client's perspective the term 'media search' has become a generic term that hides a plethora of assumptions; and this in turn creates unnecessary risk.

Pre-employment screening is about honesty, integrity and transparency and this ethos should apply equally to the relationship between a client and an outsourced screening provider. By being open and transparent as to what a particular check comprises of can only bring benefit to the relationship. The client knows exactly what they are paying for and the value of the results and the screening provider knows exactly what they are being judged against and the level of check required and media checking is a classic example of this. For this reason defining the composition of a media check is critical.

There are a variety of different methodologies that can be engaged to perform a media check in terms of pre-employment screening. Some examples are outlined below:

Lexis Nexis

Clearly one of the most established tools and repositories for the collation of media data. It is considered to be robust, extensive, largely qualified and easy to use. However the downside has always been that it is expensive to conduct research on a per click basis and therefore for many companies makes it prohibitive.

Newswire Companies

These companies scan the internet and collate and cache data (news articles, press releases, blogs etc.) that are related to particular subjects and key search streams. Invariably they provide a portal by which companies can run name searches through and results are displayed. Whilst this appears to be a fantastic solution it does invariably come with its limitations. In the majority of cases such firms are only permitted to store and reproduce information if the source of that information has declared (wittingly or unwittingly) that they are happy to share. Cases often arise where many of the newspapers, regional and national, do not permit such companies to reproduce their articles outside of their own website. This can lead to critical news stories being missed.

Google

Google remains one of the most commonly used search tools to conduct media searching. Used correctly it can be extremely powerful and reveal a host of information. The advantage of Google is that it is unrestricted on the open source internet therefore it bypasses many of the restrictive barriers. The disadvantage is that it produces thousands, if not millions of results therefore at what point do the qualification of results (against a particular individual) cease?

Specialist sites

In addition to generalist search engines there exists specialist sites and blogs that can be searched to identify particular affiliations. This may be specialist interest groups such as animal rights movements (of importance to the pharmaceutical industry) or perhaps free-lance journalist listings (prevalent to any organisation fearful of undercover journalist infiltration). These sites are by no means absolute but are valuable additions to generalist media searching.

One of the fundamental challenges in conducting a media search on a particular individual is ensuring that the results are firmly matched to the individual being searched for. When searching under common names there is likely to be a large number of results produced. In order to report a result as a match with any level of certainty a minimum of 3 key identifiers need to be satisfied. These can vary however common attributable identifiers are name, address and location, date of birth and age, known previous employer or institution, photographs etc. Similarly if the data or article was published some years previously the identifiers have to make sense to the individual at that time. Analysis of results is a skill and it also takes time. Some companies may not wish to pay for this and therefore are only interested in receiving the output. This is not necessarily wrong just as long as all parties agree that this is what is required.

The key lesson when approaching media searches within the context of a pre-employment screening requirement is to eliminate assumption and to ensure that the nature of the media check and its output is defined and clearly understood by both the client and the outsourced screening provider.

Recruitment Process Outsourcing

As The Security Watchdog's client base continues to grow, we are coming into regular contact with recruitment functions – outsourced and /or in-house. Increasingly, Recruitment Process Outsourcing (RPO) suppliers are dominating the staffing market and by the very nature of our service, we need to understand what they are, how they came into being and what benefits or risks they offer.

What is RPO?

Recruitment Process Outsourcing is a form of business process outsourcing (BPO) where an employer outsources or transfers all or part of its recruitment activities to an external service provider.

The Recruitment Process Outsourcing Association defines RPO as follows: "when a provider acts as a company's internal recruitment function for a portion or all of its jobs. RPO providers manage the entire recruiting/hiring process from job profiling through the onboarding of the new hire, including staff, technology, method and reporting. A properly managed RPO will improve a company's time to hire, increase the quality of the candidate pool, provide verifiable metrics, reduce cost and improve governmental compliance."

The biggest distinction between RPO and other types of staffing is Process. In RPO the service provider assumes ownership of the process, while in other types of staffing the service provider is part of a process controlled by the organization buying their services.

What's the History?

While temporary, contingency and executive search firms have provided staffing services for many decades, the concept of an employer outsourcing the management and ownership of part or all of their recruiting process wasn't first realised on a consistent basis until the 1970s in Silicon Valley's highly competitive high tech labour market. Fast-growing high tech companies were hard-pressed to locate and hire the technical specialists they required, and so had little choice but to pay large fees to highly specialised external recruiters in order to staff their projects. Over time, companies began to examine how they might reduce the growing expenses of recruitment fees while still hiring hard-to-find technical specialists. Toward this end, companies began to

examine the various steps in the recruiting process with an eye toward outsourcing only those portions that they had the greatest difficulty with and that added the greatest value to them. Initial RPO programs typically consisted of companies purchasing lists of potential candidates from RPO suppliers. This "search/research" function, as it was called, generated names of competitors' employees for a company and served to augment the pool of potential candidates from which that company could hire.

Over time, as business in general embraced the concept of outsourcing more and more, RPO gained favour among Human Resource management: not only did RPO reduce overhead costs from their budgets but it also helped improve the company's competitive advantage in the War for Talent. As labour markets became more and more competitive, RPO became more of an acceptable option. Furthermore, through the advent in the 1980's and 1990's of human resources outsourcing (HRO) companies that began taking on the processes associated with benefits, taxes, and payroll, companies began recognising that recruiting--a significant cost of HR--should also be considered for outsourcing. In the early 2000's more companies began considering the outsourcing of recruitment for major portions of their recruiting need.

There have been fundamental changes in the global labour market that serve to reinforce the use of RPO as well. The labour market has become increasingly dynamic: workers today change employers more often than in previous generations. De-regulated labour markets have also created a shift towards contract and part-time labour and shorter work tenures. These trends increase recruitment activity and may encourage the use of RPO. It should also be noted that even in slower economic times or higher unemployment, RPO is still considered by companies to assist in an increasing need to screen through a larger candidate pool.

What are the Benefits?

RPO's promoters claim that the solution offers improvement in quality, cost, service and speed.

Quality and Cost - RPO providers claim that leveraging economies of scale enables them to offer recruitment processes at lower cost while economies of scope allow them to operate as high-quality specialists. Those economies of scale and scope arise from a larger staff of recruiters, databases of candidate resumes, and investment in recruitment tools and networks. RPO solutions are also claimed to change fixed investment costs into variable



costs that flex with fluctuation in recruitment activity. Companies may pay by transaction rather than by staff member, thus avoiding under-utilization or forcing costly layoffs of recruitment staff when activity is low.

Service and Speed - The commercial relationship between an RPO provider and a client is likely to be based on specific performance targets. With remuneration dependent on the attainment of such targets, an RPO provider will concentrate their resources in the most effective way - at times to the exclusion of non-core activity. Traditional internal recruitment teams are less likely to have such clearly defined performance targets.

What are the Risks?

RPO can only succeed in the context of a well-defined corporate and staffing strategy. As with any program, a company must manage its RPO activities, providing initial direction and continued monitoring to assure the desired results.

Loose Definition of RPO - As RPO is a commercial concept rather than a specific definition, there is little regulation to RPO providers. As such, a recruitment agency may brand their services as RPO without actually structuring them in a way that will provide the most benefit to their clients.

Cost - The cost of engaging an RPO provider may be more than the cost of the internal recruitment department, as an RPO provider is likely to have higher business overheads.

Effectiveness - Improperly implemented RPO could reduce the effectiveness of recruitment, should an RPO provider not understand or seek to understand the recruitment solution that they will be providing.

Failure to Deliver - RPO service providers may fail to provide the quality or volume of staff required by their clients, especially when finding candidates in industry sectors where there are staff shortages.

Lack of Competition - Placing all recruitment in the hands of a single outside provider may discourage the competition that would arise if multiple recruitment providers were used.

Pre-Existing Issues - An RPO solution may not work if the company's existing recruitment processes are performing poorly, or if the service provider lacks appropriate recruitment processes or procedures to work with the client. In this situation, it is better

for the company to undergo an recruitment optimisation programme.

Employer Branding - RPO providers do not necessarily act as custodians of their clients' employer brand in the way that a strongly aligned retained search firm or internal recruiting resource would.

Engagement - Many RPO organisations perform their staffing functions and service offsite or offshore, disconnecting the provider from the client company's growth and recruiting strategy. While this effect can be mitigated through strong relationship management, some of the momentum and energy associated with the rapid upscaling of a workforce through recruitment may dissipate.

How does this impact upon Background Checking?

Background Checking sits firmly within the recruitment process. It can impact positively or negatively on each and every stage of this process and as such we are increasingly asked to collaborate closely with our client's RPO partners. This collaboration can take many different forms ranging from some very basic administrative hand-offs to full integration of process and technology.

As the labour market becomes more fluid and diverse, pre-employment screening & vetting has needed to evolve. International capability is now an absolute necessity as RPOs continue to push the boundaries and are selling increasingly complex geographic solutions. Security Watchdog has succeeded in this area where others have failed; our Subject Matter Expertise in Data Protection has exposed competitor weaknesses. The main commodity in our market is not cost or speed of turnaround – it remains the ability to give our clients absolute clarity concerning what screening can / can't be done on a global basis.

For RPOs success is gauged in many ways. Time to Hire and Speed of Engagement are key metrics. These can be hugely effected by turnaround times of the screening process and because of this it is vital that our SLAs are given due consideration when integrating with the RPO provider. Our ethos of Continuous Improvement ensures constant evaluation, efficiencies of process, the introduction of integrated technology and Straight Through Processing. All of these factors enhance the service to the RPO.

Experience dictates that the key is communication and we have proven success in delivering to our client needs in this area.

SWOT Analysis of the RPO Model

<ul style="list-style-type: none"> •Process and SLA Driven •Less time and low cost per hire <p><i>Strength</i></p>	<ul style="list-style-type: none"> •Can be a single point of failure •Expecting cost benefits too fast <p><i>Weakness</i></p>
<ul style="list-style-type: none"> •High hiring numbers across Industries •Relatively nascent service is growth markets <p><i>Opportunities</i></p>	<ul style="list-style-type: none"> •Incompetent providers •Not having a partner relationship •Other recruitment models <p><i>Threats</i></p>

If you would like to understand more about RPO and the manner in which Security Watchdog can operate in unison with RPO providers, please contact Steve O'Neil (steveo@securitywatchdog.org.uk)

NAPBS Europe to be launched in 2011

The National Association of Professional Background Screeners (NAPBS®) was founded in the US in 2003 as a non-profit trade association; NAPBS® serves to represent the interest of US based companies offering tenant, employment and background screening. NAPBS® offers an opportunity for qualified companies to participate in shaping the body of knowledge and regulations impacting our futures. NAPBS® gives the US screening industry the ability to effectively demonstrate its competence, reliability and willingness to adopt standards. NAPBS® is the best means to associate those companies able and willing to conform to standards and to meet the highest expectations of clients and law-makers. NAPBS® has adopted By-Laws, a Code of Conduct, and a Mission Statement for all members.

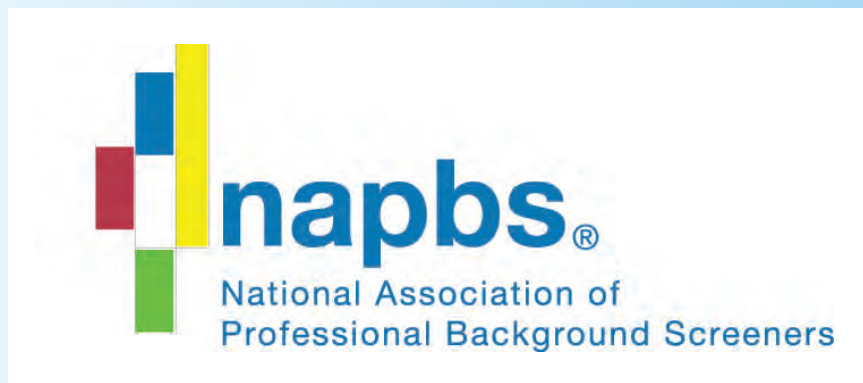
The European screening industry is still in its infancy in comparison to the US market however this means that the speed of its growth and development is far more dramatic than that of a commoditised industry such as in the US and the same can be said of the industry's dramatic growth across the Asia-Pacific region.

The need for an industry trade association within

the UK and Europe was recognised back in 2008 when NAPBS® launched their international outreach programme to encourage other regions around the world to form their own trade associations with the view of engendering wider international cooperation and education across a global background checking industry.

Since then collective meetings have been held with representatives of almost every screening firm in the UK and Europe, something that was unprecedented until this time. Their purpose was initially to agree the need for an industry trade association, something that was almost unanimously agreed, but moreover the manner in which this was going to be achieved. Following over 2 years of industry consultation the launch of NAPBS Europe is greatly anticipated. Current Co-Chairperson of NAPBS Europe, Ewan Tweedie of The Security Watchdog Advisory Bureau explains:

“I recall when our industry's organisations came together for the first time to explore the possibility of setting up a trade association for the UK and Europe. It was clear from the outset that there was great enthusiasm across the industry to make this a reality and to promote the standards and professionalism



that has become synonymous with the services provided by European vendors.

Turning a vision into a reality can often prove more difficult than first thought, especially when you have to take into consideration and balance the numerous nuances associated with screening across Europe, the different needs of the members, the expectations of end user clients and ultimately, the true objective of the association. We have liaised extensively with our colleagues from NAPBS in the US and our counterparts in the newly forming associations in Asia-Pacific and Canada. We have shared experiences and challenges in the formation of the new NAPBS chapters but I am glad that we are now in a position to formally launch in 2011.

We see NAPBS Europe playing an ever important

role in the promotion of standards across our industry, providing a platform and voice for our members to tackle the inevitable challenges we will face and to lobby government where required.

On behalf of myself and my fellow Co-Chair, Sal Remtulla of Risk Advisory Group, we would like to thank all those who have volunteered their time to play their part in the numerous discussions and steering committees over the course of the last few years.”

The industry is eagerly awaiting the official launch of NAPBS Europe in 2011 as currently the UK and European Screening Industry remains unregulated and whilst those organisations that currently represent the core industry are custodians of best practice this may not always be the case.

International Screening

AN OPERATIONAL VIEW

As Head of Division for Telecommunications at The Security Watchdog (TSW), Kellie Shapland gives her view on screening internationally.

“In a truly globalised marketplace, international screening is continuing to grow exponentially. TSW has led the way in the screening industry in terms of delivering a truly international screening service to our clients.

Having worked for the Border and Immigration Agency across EMEA from Germany to Malaysia, Russia to India, Morocco to Nigeria, I have had first hand experience working in different cultures and understanding the impact of these cultural and language differences in a business



environment. As a result I am able to combine my practical experiences together with my in depth understanding of international screening to offer real and bespoke services to my clients. As a Head of Division at TSW my clients are

predominately based within the telecommunications sector. As such we deal with high volumes of international candidates employed to work on international sites who require diverse international screening. Together with over 15 foreign language speakers on site and with an evening workforce in the UK we are able to obtain international references across the globe, whatever the language or time zone.

I am proud to be a part of a truly international screening company where my experience is of real value to both clients and TSW alike.”



DO ALL YOUR MANAGERS
KNOW WHAT TO LOOK
FOR WHEN EMPLOYING
MIGRANT WORKERS?

Immigration Watch

Interactive DVD for the prevention of illegal working

£750 +VAT

The **Immigration Watch interactive DVD** can be run from a desktop or uploaded on to your company intranet. This allows managers and recruiters to be trained to recognise the correct documents to confirm a candidate's identification and right to work documents wherever they are in the UK.

This tool is ideal for HR teams seeking to raise the awareness of a large population of individuals. For example, if you have 150 managers who regularly take copies of identity documents in the recruitment process, you could train them all on immigration rules and how to identify fraudulent documents for as little as £5 each!; a small price to pay to save expensive legal fees in the future.

To view a demonstration of the DVD or to download an order form please visit
www.securitywatchdog.org.uk/immigrationwatch

For more information contact
Ewan Tweedie, Associate Director
tel: +44(0)1420 593832
email: ewant@securitywatchdog.org.uk

The Security Watchdog Advisory Bureau
Cross and Pillory House, Cross and Pillory Lane
Alton, Hampshire, GU34 1HL