

# **BACKGROUND SCREENING BEST PRACTICES:**

*Insights from Accredited  
Background Screening Firms*

BEST  
OF THE  
BEST



**PreemploymentDirectory.com**



# A Cheap Background Check Cannot Defeat a Maze of Deception.



Finding the truth in today's digital world requires more than running a few databases. Savvy job candidates concoct false identities, create fake educational credentials and invent fictional references. At RAI, our investigators work through the maze of deception to produce a thorough and comprehensive investigative report. The path to the truth is not accomplished by cutting corners.

**There is a difference between a background “check” and a background investigation.**



Discover the RAI difference at: [www.raiglobal.com](http://www.raiglobal.com)





# IT'S NOT SEXY!



But, Background Screening Is An Important Hiring Tool To Help You Hire People With The Skills You Want And Avoid Bad Hires.



## PREEMPLOYMENTDIRECTORY.COM

"The Information Portal for Background Screening"

# TABLE OF CONTENTS

Article Title	PG
1. The Journey to Earning Accreditation .....	4
2. What Constitutes a Thorough Background Check .....	5
3. Employers: Are You Paying Attention to What Comes After the Background Check?.....	7
4. Employers – Are Your Background Screening Consent Forms a Liability? .....	9
5. NAPBS Accredited Background Screening Agency: Why It Matters .....	11
6. Best Practice Guide to Choosing a Background Screening Partner.....	13
7. Are You Performing Background Checks or Background Investigations? The Difference is Critical to the Success of Your Business.....	16
8. Information Security a Top Priority for Background Screening Firms Due to Recent Data Breaches .....	20



## ABOUT US

PreemploymentDirectory.com is the most comprehensive web based directory of firms in the background screening industry. It is designed to make it easy for organizations to quickly find information about background screening or a screening company to meet their needs.



The Directory is an essential resource for Human Resources and Hiring Managers looking for background screening resources.

The Directory consists of several sections to quickly guide organizations to find the information they need or a company that will serve them best:

- The U. S. Domestic Section includes background screening firms (CRAs) listed by the location of their headquarters on a State by State basis.
- The International Section includes firms that conduct background screening on candidates who have lived, worked or been educated in a country other than the U.S. These firms are listed by country.
- A Background Screening Knowledge Center which has an extensive Article Library, U.S. and International Resource Centers, results of our annual Employers Background Screening Practices survey, a calendar of events and much more.

In addition, we are the leading publisher for the background screening industry. Available Publications include:

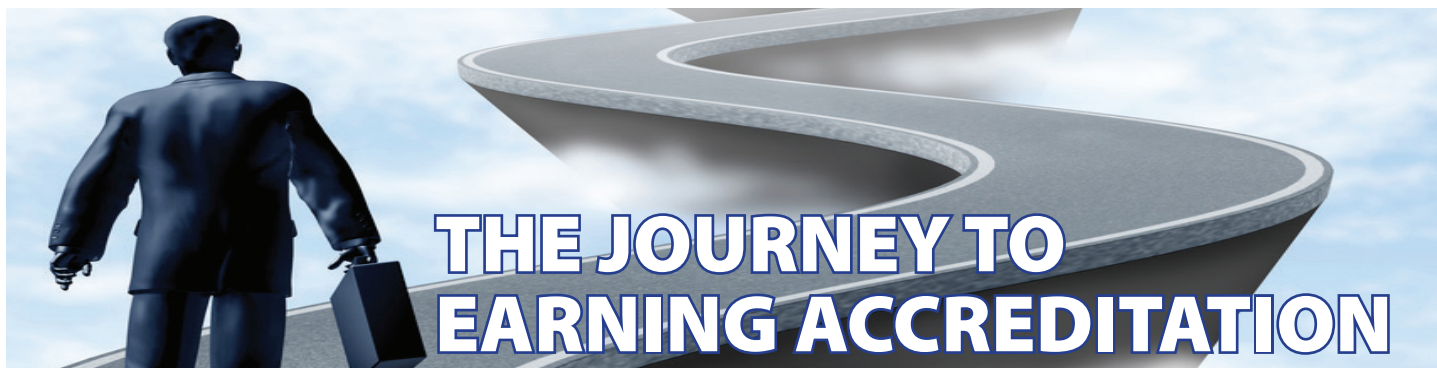
- The Background Buzz. The award winning and leading online newsletter for professional background screeners.
- The Global Background Screener, an award winning e-magazine for the worldwide background screening industry.
- 2016-17 Annual Background Screening Industry Resource Guide
- 2016-17 Annual Suppliers to the Background Screening Industry Buyers Guide
- Background Screening Best Practices: Insights from Accredited Background



# PREEMPLOYMENTDIRECTORY.COM

"The Information Portal for Background Screening"





Background Screening firms can be accredited through the National Association of Professional Background Screeners (NAPBS). The process is overseen by the Background Screening Credentialing Council (BSCC), which certifies that background screening firms follow the Background Screening Agency Accreditation Program (BSAAP) Standard. This process ensures companies comply with relevant laws, ethical business practice and demonstrates a commitment to excellence.

### **Before a Company Can Submit an Application**

---

In order to qualify for accreditation, a background screening firm must be regularly and primarily engaged in the business of providing employment screening services to qualified firms, generally referred to as end-users.

The firm must have been providing services under the BSAAP Standard for at least a year before filing the application for accreditation. This allows the firm time to establish documentation of their compliance in all procedures, which will be reviewed as part of the accreditation process. It's not sufficient to merely reflect the standards in official policies. It must also be demonstrable in daily business operations.

The firm must have responded to any and all NAPBS and BSCC complaints or grievances before beginning the application process.

A Letter of Intent to Apply for Accreditation Form should be submitted at least six months before the official application is submitted.

Would-be applicants should have all materials in order before applying for accreditation. If an auditor finds serious shortcomings, the application may be denied. A denied firm must wait a full year before reapplying, at which point fees will again need to be paid and all paperwork will need to be updated and submitted.

### **Application and Initial Auditing**

---

At the appropriate time, the firm should submit the application and required fees. Once the firm's eligibility is confirmed by the BSCC, they are given six months to complete a self-evaluation.

An independent auditor will then review both the application and the self-evaluation, potentially requesting further clarification or materials from the firm. The review may include (and shall not be limited to):

- |  |                                       |
|--|---------------------------------------|
| • <i>Required policies and procedures</i>                | • <i>Sample conformity documents</i>  |
| • <i>Copies of cover pages of required documentation</i> | • <i>Client and vendor agreements</i> |
| • <i>Job descriptions and resumes</i>                    | • <i>Training materials</i>           |
| • <i>Required evidence of use of BSAAP Standard</i>      | • <i>Client education materials</i>   |
| • <i>Security plans</i>                                  | • <i>Proof of insurance</i>           |

The independent auditor will also perform an onsite review of the firm, confirming the firm has put the BSAAP Standard into everyday practice.

The independent auditor will then submit an Audit Findings Report to the firm within two weeks of the onsite audit. The firm has ten business days to respond with any final necessary documentation and clarifications.

### **Gaining Accreditation**

---

The independent auditor submits a full report to the Council, which will make a final decision on the application. The firm will be notified within ten business days of the decision. Once approval is received the accreditation is valid for five years. An Interim Surveillance Audit by the independent auditor is required before the end of the third year.

These strict enforcements of guidelines provides heightened protections to organizations and predictability of the type of services that will be offered as well as enhances the credibility of the background screening profession. Using an accredited background screening firm is an all-around winning situation for any organization.

Source: The information in this article is our summary of the NAPBS accreditation process and was not written by NAPBS. For detailed and specific information on the accreditation process visit [NAPBS.com](http://NAPBS.com).



# WHAT CONSTITUTES A THOROUGH BACKGROUND CHECK?

*By Christine Cunneen, CEO of Hire Image, LLC*

Contrary to popular belief, many states don't submit criminal records to national databases, and many only provide incarceration records. With the absence of a true national criminal database, the best option is hands-on research at the primary source: local county courthouses. With over 3,000 counties in the U.S. and over 10,000 courthouses storing criminal records, it's impractical to search a person's criminal history in every courthouse.

This is why a comprehensive background search begins with **address and social security number research**. An address and SSN trace can reveal alias names as well as addresses where the applicant has lived, typically over the last 7-10 years.

**State repository and/or database searches** are a valuable supplement to county courthouse searches, allowing for a broader investigation and identification of an applicant's criminal past outside of the counties of residence. However, information obtained may be outdated or incomplete. A county criminal search should be conducted to verify the information and final disposition.

**Federal criminal searches** uncover law violations recorded in U.S. Federal District Courts. Such serious crimes may involve embezzlement, robbery, drug trafficking, mail fraud, racketeering, crimes over the Internet, and kidnapping.

Many employers erroneously trust the **FBI fingerprint identification database** as the "gold standard" in background screening. In reality, this is a tool to be used but **not reliable as a single source for a background check**. Federal law or state statute must require the FBI check, and employers should be aware of potential pitfalls of using the system.

Additional search recommendations include terrorist watch lists and verifications of education, employment and professional licenses. Credit reports, driving records and drug testing are also valuable screening tools.

The Fair Credit Reporting Act (FCRA) requires an employer to provide written disclosure for background screening investigations, and receive prior authorization from the applicant. If an employer chooses not to hire, additional rules must be followed including providing the applicant with a pre-adverse action letter (sent with a copy of the screening report and FCRA summary of consumer rights) followed by an adverse action letter after a reasonable period of time.

Before making the decision not to hire an applicant with a negative background screening report, the employer should also address EEOC Title VII considerations and specific state rules. Consult an employment attorney to ensure compliance with all federal and local regulations.

Employment screening can be vital to your company's overall success. Ignoring it or performing cheap, substandard searches can cost your company a lot more than the price of a comprehensive screening process.

## About The Author



Christine Cunneen is the CEO of Hire Image, LLC. She is the Immediate Past Chair of the National Association of Professional Background Screeners (NAPBS), and also holds Advanced FCRA Certification through NAPBS. She is a member of SHRM, serving on the advocacy team and legislative committees. Cunneen is a frequent speaker at events educating employers and other professionals about background screening and is often quoted for her expertise in the news media. She travels to DC often to meet with legislators and is involved in advocacy pertaining to laws and regulations that impact hiring practices and the background screening profession.



30% of all business failures are caused by employee theft;  
355,000 businesses will have an episode of violence in the workplace;  
80% of employee turnover is due to bad hiring decisions\*

# Can you afford *not* to use HireImage?

Background screening specialists

## The Hire Image difference:

- NAPBS Accredited
- U.S. owned and operated – no offshoring
- Woman-owned company
- Fastest turnaround times
- Secure online system available 24/7/365
- Fully staffed LIVE customer service
- All operational staff FCRA certified
- SHRM Recertification Provider

## Check out COMPLY<sup>SM</sup>

*Our proprietary method to remind employers of their compliance obligations.*

**C**andidate notification (stand-alone disclosure)  
**O**btain candidate's signed authorization AND provide  
**M**andatory FCRA summary of rights and state disclosures  
**P**re-adverse notification (if applicable)  
**L**eave time for candidate to dispute  
**Y**ou decide: Hire, or Not (send adverse action letter)

## NEW 2016 Compliance Guide to Background Screening

- Latest information impacting background screening
- Keep up with changing national, state and local laws
- Regularly updated
- FREE, available in PDF format



**FREE compliance review and FREE Compliance Guide.**

**Contact:** [comply@hireimage.com](mailto:comply@hireimage.com) • 888-720-HIRE (4473)

[www.hireimage.com](http://www.hireimage.com)

Corporate Headquarters: 6 Alcazar Avenue, Johnston RI 02919  
Regional Offices in Florida, Minnesota, Washington and Wisconsin



This information is provided for educational purposes only and is not legal advice.

\*Sources: U.S. Chamber of Commerce; Society for Human Resource Management; Academic and Business Research Institute.



# OFFER OF EMPLOYMENT

---

## ARE YOU PAYING ATTENTION TO WHAT COMES AFTER THE BACKGROUND CHECK?

*By Heidi Seaton, VP Operations and Compliance*

Many employers are familiar with requirements around making disclosures to applicants and getting their authorization to do a background check, but employers continue to miss the essential final step of the process. If an employer decided not to hire an applicant based on the content of the background report, the federal Fair Credit Reporting Act (FCRA) requires that the employer follow a multi-step “adverse action” process:

**Step 1: Pre-Adverse Action** - the employer must provide the following information to the applicant before the adverse decision is made:

- Provide written notice to the applicant that the employer is considering making a negative hiring decision (the content of this notification is defined by the regulation),
- Provide a copy of the background report that the employer is using to make the decision, and
- Provide a copy of the “A Summary of Your Rights Under the Fair Credit Reporting Act” document, published by the Consumer Financial Protection Bureau
- A number of states and counties now also require additional disclosures, and in some cases, information be provided to the applicant about the specific information in the consumer report that the employer is considering.

**Step 2: Wait** – the employer must wait a “reasonable” period of time for the applicant to receive the notification and notify the employer (or the background screening company) that they intend to dispute the information in the background report. The regulation does not define this time period, however regulators and courts have weighed in, and now generally an employer would want to wait no less than five business days. In addition, employers will want to carefully review Ban-The-Box legislation in their hiring locations, as such regulations (for instance in New York City) can require a longer waiting period.

**Step 3: Final Adverse Action** – If, after the waiting period and any subsequent dispute from the applicant, the employer still intends to make the decision final, the employer must send the applicant a Notice of Adverse Action informing the applicant that the employer has made a final decision, along with another copy of the “A Summary of Your Rights under the Fair Credit Reporting Act” document. The content of this second notification are also defined by the regulation. Again, check local Ban-The-Box legislation to determine whether additional state or local additional disclosures are required.

*The foregoing is not legal advice, either expressed or implied. We recommend you seek the advice of your corporate legal counsel for all aspects of employment law.*

### About The Author

---



Heidi Seaton is Orange Tree’s VP of Operations and Compliance. Heidi has been in compliance in the background screening industry for fifteen years and was the project lead for Orange Tree’s achievement of NAPBS Background Screening Agency Accreditation in 2011. She earned both her NAPBS “Basic FCRA” Individual Certification in 2012 and the NAPBS “Advanced FCRA” Individual Certification in 2015. In addition, Heidi is the current Co-chair of the NAPBS Best Practices committee.





Turn hiring into a  
source of security  
and assurance

**Orange Tree. Hire with Confidence.™**

Employment background screening  
solutions for you, your candidates  
and your company



**CONTACT US**

1.800.886.4777

[salesteam@otes.com](mailto:salesteam@otes.com)

[www.orangetreescreening.com](http://www.orangetreescreening.com)



## EMPLOYERS – ARE YOUR BACKGROUND SCREENING CONSENT FORMS A LIABILITY?

*By Sebastian Dehnel, Vice President of Operations*

Before an employer can conduct a background check on a job applicant, it must provide a disclosure to the individual explaining that a background check will be performed. It must also obtain written consent from the individual. Sound easy? Perhaps it is not. In 2015, over 25 class action cases were filed against some of the largest employers in the United States accusing them of conducting background checks with invalid disclosure and authorization materials. These cases have resulted in shockingly large settlements ranging from \$500,000 to \$8,000,000.

### What Theory Are Plaintiffs' Attorneys Advancing?

The bulk of the attacks on employers' written consent materials focus on the background screening "disclosure. This is because the Fair Credit Reporting Act (FCRA), the federal law governing background checks, imposes some technical (but sometimes ignored) requirements. More specifically, the FCRA states:

"A person may not procure a consumer report, or cause a consumer report to be procured, for employment purposes with respect to any consumer" unless a "clear and conspicuous disclosure" has been made in writing to the consumer" "in a document that consists solely of the disclosure" stating that a "consumer report may be obtained for employment purposes."

Employers are frequently getting sued because they are allegedly including too many items in the "disclosure" or combining the "disclosure" with other employment materials. According to plaintiffs' attorneys (and some judges), including unnecessary items in the disclosure or combining the disclosure with other documents renders it invalid. An invalid disclosure means an invalid background check.

### What Can Employers Do to Protect Themselves?

The "old days" of ignoring what goes into background screening consent materials are over. In this new era, employers ought to be working closely with counsel to ensure that their written consent materials are fully compliant. The primary goal is to ensure that the disclosure does not have items that could be considered "extraneous." Below are some examples:

- a. Releases of Liability stating that the employer and/or screening company will be held harmless for any background screening requests or mistakes.
- b. State law notices explaining the consumer's rights under various state statutes, as opposed to the Fair Credit Reporting Act.
- c. Statements suggesting that the consumer's employment with the company will be "at will."
- d. Statements suggesting that the applicant understands that the employer does not discriminate against applicants/employees.

Further, employers should double-check that their disclosures are not combined with other materials such as a job application or employee handbook. This too can violate the FCRA's "stand alone" requirement. Put simply, background screening compliance is no longer a "back burner" issue. Identifying experienced counsel and background screening providers, and reviewing screening procedures, is more important than ever before.

### About The Author



Sebastian Dehnel is Vice President of Operations at CriminalRecordCheck.com, a full service background screening provider based in Raleigh, NC. He has worked in the background screening industry for over 13 years and is a licensed North Carolina Private Investigator (NCPI 4121). As an active member of the NAPBS Sebastian serves as Chair of the Best Practices Committee and was one of the first 30 people to receive the NAPBS Advanced FCRA Certification. Sebastian graduated from East Carolina University with a BS in Business Administration.





# *SCREEN WITH CONFIDENCE*

CRC is an established and credentialed background screening firm offering customized solutions to meet your exact needs. CRC clients experience industry leading customer service, turnaround times, and compliance support. All CRC Staff are FCRA Certified and our technology has unique capabilities to expedite compliance fulfillment. Accreditation by the NAPBS reinforces our commitment to consumer protection, data security, and operating at the highest industry standards. Call us today...experience the CRC difference!

## **MULTIPLE ORDERING METHODS**

- ATS Integrations
- Applicant Driven
- Batch Ordering
- Order by SSN

## **INTEGRATED SUPPORT**

- Federal, State, and Local Compliance
- Document fulfillment

## **CUSTOM DEVELOPMENT**

- Tools that meet your exact needs

**CriminalRecordCheck.com**

PO Box 90998 | Raleigh, NC 27675-0998  
Toll-Free: 877.272.0266 | Fax: 800.650.5992



# NAPBS ACCREDITED BACKGROUND SCREENING AGENCY: WHY IT MATTERS

*By Michael Gaul, Executive Vice President, Marketing*

The National Association of Professional Background Screeners (NAPBS) offers an accreditation program for businesses located in the United States of America. Governed by the Background Screening Agency Accreditation Program (BSAAP), the program has become a widely recognized seal of approval that confirms an organization's commitment to excellence, accountability, high professional standards, and continued institutional improvement. Only companies with a deep commitment to these principles are qualified for NAPBS accreditation. Proforma Screening Solutions is honored to be one of those companies. This accreditation puts us among fewer than 10% of NAPBS member organizations that have earned the accreditation. For you, our accreditation means you can feel even more confident in our ability to deliver screening results that are legally compliant and verifiably accurate.

## Our Promise to You

You face a daunting challenge to find good employees—and to avoid risky ones—while staying within the fence created by legal requirements. To this end, background screening is an essential tool. The NAPBS accreditation program aggregates background screening best practices in a demanding process that helps you know that the screening-based employment decisions you make stem from sound research and reporting practices.

*The BSAAP for Consumer Reporting Agencies (CRAs) covers:*

- Data security,
- Legal compliance,
- Client education,
- Researcher and data standards,
- Verification services standards, and
- Business practices.

Within each of these categories, the standards require companies to identify role-based responsibilities, establish effective written policies and procedures, train employees as needed, monitor, and make changes as needed. The entire process is built around ensuring that the agency communicates legal requirements to clients and that clients understand the role of the CRA in the background screening process.

We are proud to qualify as an accredited background screening agency under these standards and look forward to continuing to serve you with confidence.

## About The Author



Proforma Screening Solutions delivers a wide-range of background checks and background screening services to help companies make better hiring decisions. We provide employment background checks to companies large and small - all with the common objective of helping organizations select the right people, the first time. The right background check company will play an important role in your ability to select and retain the right people for your organization. As a

security industry professional since 1988, Michael Gaul has extensive expertise in the fields of human capital risk management, physical security, and background screening process management. Michael leads Proforma's marketing and strategic customer relations efforts.

For more information about Proforma Screening Solutions, please contact them at (866) 276-6161, [Talk@proformascreening.com](mailto:Talk@proformascreening.com) or [www.ProformaScreening.com](http://www.ProformaScreening.com)



# Reduce Your Hiring Risks

Make better hiring decisions and maintain compliance with comprehensive employment screening solutions from a partner you can trust.



**Proforma**  
screeningsolutions®

CRIMINAL RECORDS | VERIFICATIONS | DRUG SCREENING | MORE

Get started.

[ProformaScreening.com](http://ProformaScreening.com)  
(866) 276-6161





# BEST PRACTICE GUIDE TO CHOOSING A BACKGROUND SCREENING PARTNER

*Robert Capwell, Chief Knowledge Officer, Employment Background Investigations*

The crucial task of selecting a trustworthy background screening partner can be a difficult one, and options continue to grow as the industry expands and technology evolves. Your background screening partner is a key component of your talent screening and selection process, so finding the right partner with the right fit for your screening program is paramount. That partner should support your hiring process by delivering timely, accurate, and compliant information of the highest quality while delivering industry leading customer service. This guide was created as a best practice resource to help you make this big decision.

## **Expertise and Length of Experience**

The background screening profession has evolved dramatically over the past two decades. Some of the biggest changes are in the legal landscape, technology, and service offerings. You need a partner that is experienced and exhibits a long-standing reputation in the field. Conduct some online research and look for evidence of thought-leadership over time. A knowledgeable screening firm will share information and resources directly on their site by publishing white papers, articles and blogs. In addition, conduct research on the firm's leadership team, this will provide solid insight into the expertise of the firm's executive management team.

## **Industry Involvement and Credentials**

Industry related associations represent the nucleus of education, best practice, advocacy, and industry governance. The background screening industry is no different. The National Association of Professional Background Screeners (NAPBS) is the global voice and guiding association of the screening industry. Association involvement provides critical resources to stay current with the ever-changing legislative landscape, compliance mandates, best practice techniques and new solutions. NAPBS members better understand information privacy and security, advancements in screening technology and available resources. In addition, the association fosters certification programs for members to test and show their knowledge of FCRA compliance.

Companies prove their commitment to industry best practices and standards by becoming accredited. Only a small number of companies are accredited through the NAPBS Background Screening Agency Accreditation Program. Accredited firms demonstrate their diligence and dedication to their clients through solid performance in crucial areas such as information security, legal compliance, client education, research and data standards, verification standards and overall business practices. Each is vetted thoroughly by an independent auditor before receiving the accreditation badge of excellence. A commitment to accreditation is a pledge to the background screening industry and ensures employers receive the highest quality of information while serving the best interests of candidates through privacy and compliance.

## **Service Capabilities and Your Customized Needs**

The benefits and risk reduction strategies demanded of a background screening program are unique to each employer. Company size, structure, industry, and job description are all key factors that play into the decision-making process. Trying to fit every screening program into the same mold will not work. You need to rely on a screening partner that can walk you through all of the

options. Custom packages that are specific to a particular job function will provide the best benefit and value for your program. HR professionals who oversee several decentralized locations can leverage automation to receive consistent screening while ensuring compliance with company policy, as well as state and federal laws.

Employers hiring internationally will require a partner that has an in-depth knowledge of international screening protocols. Consolidating services such as background screening, drug testing, occupational health screening solutions, E-Verify and paperless I-9 compliance requirements can save time and money. The use of multiple software platforms, managing multiple vendors, and reconciling several invoices is not an efficient use of your time. A one-stop solution partner can consolidate management reporting, provide for a consistent program review and provide opportunities for additional savings based on consolidated volume.

### **Technology that Supports Business Optimization and Your Onboarding Process**

Your background screening program should fit strategically within your hiring and onboarding process; not be held at the mercy and convenience of your screening partner. A seamless integration with your provider can optimize your hiring process and save you considerable data-entry and processing time. Leveraging the use of a self-serve applicant kiosk or electronic portal can make the application process integrated, virtual and candidate friendly.

A seamless integration with your screening partner can securely route candidate data, paperless forms, and an e-signature process from your applicant tracking system through to your screening partner and back to an HRIS system. Compliance can be achieved virtually too with the use of service specific disclosures, federal, state and internationally required notifications and forms. All can be served up automatically as need and then executed using an electronic mouse signature technology. A paperless storage environment makes it easy to retrieve information and maintain proper compliance.

### **Client Onboarding, Training, and Program Reviews**

The day you sign the contract with your new provider shouldn't be the last time you hear from them. Establish the process for onboarding, training, and program review upfront to ensure a smooth transition. Also, outline how you will measure the success of your screening program.

Background screening technology platforms can be very customizable these days. Once you determine what you need, you can start setting the parameters to fit your needs. It is essential to decide who is authorized to request and review screening results. For multi-location users, this piece is paramount to ensure legal compliance and proper setup for management administration and review.

Training is an integral part of the onboarding process. Be sure that your provider offers customized live training to address specific training needs and questions before the program starts. Ongoing training should also be available for future users, and insist that your partner provides resource material and training documentation for future reference. Discuss the option of scheduled program reviews. The success of your screening program should be benchmarked and measured on an ongoing basis. Establish key performance indicators (KPIs) upfront and measure them on a periodic basis to track performance. Management reporting and subsequent reviews are great measures to determine program success.

### **Approach and Structure to Account Management and Customer Service**

Customer support is a key component of a successful screening program. The level of support varies from company to company. You should have a firm understanding of the support team working with you and how they gauge your satisfaction. Will you be assigned an individual account representative, and is there a support team working with them for strategic account administration? In addition, you should ask about the structure of their customer service team, off-hours support and the use of overseas call centers to make sure they meet your specific support needs.

### **Quality Management and Customer Satisfaction**

Background screening firms concerned with quality and customer satisfaction take strategic measures to incorporate a quality management system into their core operating principles. A successful quality management system will include documented procedures and training for each business function. The firm should be measuring specific inputs and outputs as they relate to each function within the process. Benchmarking and measurements around timeliness, accuracy, compliance and your satisfaction should be measured and reviewed on a constant basis. This is used to gauge quality and your level of overall satisfaction as a basis for continual improvement. Decide what quality and overall satisfaction means to you and what key performance indicators will be used to measure your program's success. A background screening firm dedicated to quality will have a comprehensive program



already in place. The customer service team should continually seek your feedback and act on that information to increase overall quality and your satisfaction.

### **Data Privacy, Security and Business Continuity**

The background screening process involves the processing, handling, and storage of a candidate's sensitive information. The concern over data privacy and protecting personally identifiable information (PII) is real in today's landscape of growing identity theft. Background screening firms that are focused on data security incorporate strict measures in all facets of information security. Be sure your trusted screening partner already has a security policy, information security procedures and training, documented procedures to deal with security incidents, access control policies and risk mitigation strategies to ensure business continuity.

Legislation concerning data privacy is ever-changing and must be monitored for constant compliance. Be sure your provider has a solid grasp of both international and domestic data privacy and security. A concerned partner will follow the new Privacy Shield Framework to comply with the European Union Commission's Directive on Data Protection. In addition, concerned partners will not offshore sensitive client and candidate data overseas. Once sensitive data leaves the United States, there are no guarantees of data protection or secured access to PII. No employer wants to be burdened with the liabilities of an applicant's data being mishandled.

### **Responsible Use of Database Information**

Criminal record searchers are available in a variety of government and privately held electronic databases. This information can be alluring to employers that want to save money and time. This type of information is a critical research tool; however it should never be used as a sole source of data to conduct a criminal background check.

The quality of a criminal records database will vary from source to source with no guarantees of data quality or even significant identifiers to match your candidate. Good background screeners verify criminal records data from the original reporting court to ensure current and reportable information within the legal guidelines of the Fair Credit Reporting Act (FCRA). Using unverified data to make a hiring decision can create additional liabilities for employers and a very unpleasant candidate experience.

### **Compliance Resources and Support**

Legal compliance within the background screening industry is ever-changing and opens up potential liability for employers if not followed closely. The Fair Credit Report Act (FCRA), state local, and international laws must be followed for proper compliance. Your background screening provider should be your resource for a compliant screening program.

Your partner should provide documentation such as authorization and disclosure forms.

Laws can differ county to county, state to state and even country to country. Your partner should provide resources and guidance to make sure your program is compliant at all times. Be sure to speak with your representative about how the company will provide mandatory compliance information and how legal changes will be made. Your provider should have a compliance team that is focused on current compliance protocols and keep their pulse on ever-changing legislation that could affect your screening program.

### **Conclusion**

Conducting proper due diligence on your potential screening partner, and addressing the topics provided within this guide, will ensure that the provider you choose has the capabilities and expertise to handle your customized needs. A suitable partner will understand quality, information security and have the technology to optimize your program. Establishing a relationship based on specific measurements of mutual success will establish a program that is seamless, cost-effective, efficient, and compliant.

## **About The Author**

---



Chief Knowledge Officer Mr. Robert E. Capwell is considered one of the leading experts in the background screening industry with over 24 years of experience in the field. Employment Background Investigations, Inc. (EBI) is a technology driven leader in domestic and global pre-employment background checks, drug testing, occupational health screening and I-9 compliance. EBI specializes in development, implementation and management of customized employment screening programs for large and multi-national clients. EBI is dedicated to information security and is the only NAPBS Accredited background screening company to hold both an ISO 27001:2013 certification for information security and an ISO 9001:2008 certification for Quality Management.



# **ARE YOU PERFORMING BACKGROUND CHECKS OR BACKGROUND INVESTIGATIONS?**

## **The Difference is Critical to the Success of Your Business**

*By: Kevin Prendergast, President and General Counsel*

The candidate's credentials were outstanding. Undergraduate and graduate degrees from a prestigious university. He presented an exceptional work history with long-term management positions at two Fortune 500 companies. He had a clear criminal record in the area where he lived for over twenty years. There was just one problem. It was all a lie.

The candidate had applied to become the VP of IT Security at our client, a prestigious professional service firm. He was offered the position contingent on a successful background investigation. He interviewed well and the hiring managers liked everything about him. He was brought on board to fill a critical need before the background investigation was complete. The hiring turned out to be a mistake.

In this article, we will discuss the important difference between a background "check" and a background investigation. The true case of the IT candidate mentioned above will be used to illustrate the importance of going beyond a superficial inquiry when screening employees, especially those applying for key positions within your organization. The example discussed throughout this article is not an anomaly. The concerns raised by this one case are issues my firm sees every day as candidates lie and embellish their credentials to obtain positions for which they are unqualified. Unfortunately, for many employers performing superficial background checks, the concerns would never have been uncovered by a basic background check and often lie dormant until a serious issue arises post-hire.

### **The Cost of a Bad Hire**

The U.S. Chamber of Commerce estimates that theft by employees costs American companies \$20 billion to \$40 billion a year. The chamber also reports that an employee is 15 times more likely than a nonemployee to steal from an employer. Most of the perpetrators of these crimes against employers did not have a previous criminal record. Yet many employers believe a cheap and quick criminal background check is sufficient to combat employee theft. Unfortunately, they are relying upon information that is minimally predictive of the conduct they seek to curtail.

In addition to relying upon the wrong information, employers often get wooed into a false sense of security since the majority of candidates have clear criminal histories. Since the vast majority of criminal background checks come back clear, some employers fall into the trap of believing that candidate vetting is little more than a formality that can be accomplished with some quick database searches and a basic criminal background check. For the professional service firm discussed earlier in this article, their clear rate was at 98%. But they realize that background screening is not about clearing the 98%. It is about avoiding the 2% that can wreak havoc in your organization. And those 2% of candidates are capable of some incredible deception.

In over 50 years of conducting background investigations, my firm has found that deception can take many forms. It may provide some comfort to know your candidate has a clear criminal record. But it is equally important to determine whether a candidate has falsified their education or employment history. This will help ensure both their professional qualifications and their integrity. Avoiding employee theft and criminal behavior are important objectives to a background screening program. But equally important is ensuring that the individual possesses the requisite skills and qualifications to do the job they are hired to perform. Unqualified and incompetent employees cost employers dearly since those employees rarely work out, can damage a client relationship and require significant resources to fix the problems they cause.

A recent study indicates that a problem employee will cost his or her employer 125% of their annual salary. This figure includes: (1) amounts paid to the employee for salary and benefits; (2) recruiting and training costs; (3) management time dealing with “the problem;” and (4) termination costs and replacement expenses. Assuming one in every 20 job applicants is ill-qualified, consider this example of the potential ROI of a comprehensive background screening program:

#### **Administrative Employee.**

- \$28,000 Annual Salary.
- 125% of Salary= \$35,000
- Cost of comprehensive BI \$350

#### **Professional Employee**

- \$80,000 Annual Salary.
- 125% of Salary= \$100,000
- Cost of Comprehensive BI \$500

A comprehensive background investigation will go well-beyond a database check or mere criminal history search. An in-depth background investigation will verify the applicant’s educational credentials, employment history, professional licenses and other pertinent information. But obtaining that information is just the start. Unlike a background check, a true investigation will not only obtain this data, it will dig into conflicting and discrepant findings and take the extra steps to uncover the truth. As illustrated above, the cost for these in-depth searches are typically one percent or less of the cost of one bad hire.

#### **The Cell Phone Deception**

Mobile phones have become an indispensable tool for both personal and business life. They are also an instrument for deception. An investigator can never assume that the party on the other end of a cell phone call is legitimate.

Our IT candidate discussed above had provided two employment references from his previous employers and their cell phone numbers. The references confirmed his management-level titles, dates of employment and provided glowing remarks about his job performance. However, the official company records did not confirm either employment.

When confronted with this discrepancy, the candidate pushed back. He claimed that the HR records were incorrect. He produced real-looking payroll records and an offer letter from each company. The hiring manager was satisfied. The HR professionals were not. Our investigator dug deeper.

The profiles for the two references and the job candidate were accessed through an on-line source. The employment history on the references’ profiles did not show that they had worked with the applicant at the companies where employment was claimed. Rather, the three had worked together at a start-up company a few years earlier. Employment records were also negative for the references at the firms where they claimed to work. Neither of the references nor the applicant had ever worked at the firms.



Accepting cell phone verifications is acceptable to some lesser background screening firms. However, nothing short of an official verification through the company should be accepted. There is no way to really know who is on the other end of a cell phone and these phones can be obtained easily and inexpensively. We are seeing this type of deception more frequently and counsel our clients not to accept this information without an official verification directly from the information source.

### **The Educational Fraud**

Fake diplomas can be created on a laptop and cheap printer in minutes. The same is true with educational transcripts. We regularly see fake documents from candidates who claim degrees that were never obtained.

When our investigator attempted to verify the undergraduate and graduate degrees for the IT candidate, she was advised that there was a financial hold on the applicant's records for failure to pay a bill- from 1993. Because of this, the university was refusing to provide any information regarding the applicant. The degrees could not be confirmed. When confronted with this information, the applicant produced official looking transcripts and a copy of his diplomas showing both degrees. He even produced a recent background check from a lesser firm that verified the educational history based upon his transcripts and diplomas. Our investigator was not convinced.

The investigator contacted the university and asked to speak directly with the registrar. The situation was explained and the investigator offered to forward the documents at issue to the registrar for verification. The issue was presented not as an educational verification but rather a check into whether there had been academic fraud. The registrar agreed to review the documents and immediately contacted us after his review. The documents were fraudulent. The applicant had been getting away with a lie for over 20 years by refusing to pay a bill and thereby blocking access to his academic records.

Unfortunately, educational fraud has become more common as the job market has tightened. Candidates are willing to take a chance and lie since there is often no penalty for getting caught. Without our investigator taking the extra steps and looking through what the candidate presented, this candidate may have been hired into an IT security position. A cheap background check would not have discovered these issues. A background investigation uncovered the truth.

### **The Undisclosed Address**

During the course of the investigation, an address history was developed for the applicant showing an address in New York for most of his adult life. But an odd address popped up in another state. The odd address could have been easily ruled out since the applicant had a common name. A cheap provider would have ignored the address. When confronted with the address, the applicant denied any connection.

Applicants will often fail to disclose an address where a problem arose so as to avoid detection of that problem. In this case, the out-of-town address was checked and a criminal record was found. The record indicated that the defendant was part of a scheme of stealing laptop computers from his employer and then selling them on-line. However, the on-line court data did not reveal any identifiers for the defendant.

Better investigative firms will have a national network of affiliates who can go to the various court repositories and obtain records. We contacted our field representative who went to the court and copied the criminal file. Deep in the court records, we found a social security number, date of birth and a signature of the defendant on a plea agreement. The identifying information was matched to the applicant and the signature was matched to onboarding documents that the applicant had executed when hired. Incredibly, the applicant was still on active probation from the criminal case and was making monthly restitution payments.

Obviously, our client removed the employee from his position. Certainly, the recent criminal case was enough to deny this individual employment. But the education fraud and fictional employment history provided grounds to take adverse action as well.

Unfortunately, many companies still believe that background screening is an area to cut corners and go cheap. Quick and dirty background checks can be performed on-line with little or no interaction between the company and the screening firm. But a savvy candidate can easily defeat these background checks because basic checks are not designed to uncover fraud and deception. What a company saves in utilizing the services of a cheap provider is easily lost in one bad hire.

There is a difference between performing a background check and conducting a background investigation. If a company is not performing thorough investigations, they are missing quite a bit of information. Additionally, a better firm will provide compliance support to assist employers through the tangled web of federal, state and local laws regulating background investigations. At RAI, we have developed an on-line platform which manages the compliance process for our clients, including all of the necessary documents for initiating an investigation, conducting adverse action and handling applicant disputes.

### About The Author

---



Kevin P. Prendergast is the President & General Counsel at Research Associates, Inc., a corporate investigative firm serving clients since 1953. Kevin oversees the compliance program at RAI and works with clients and their counsel in developing legally compliant background screening programs. Mr. Prendergast graduated from the Cleveland

Marshall College of Law and has been licensed to practice law since 1987. He is a member of the Society for Human Resource Management, the American Bar Association, the Ohio State Bar Association and the National Association of Professional Background Screeners. He holds advanced FCRA certification from the NAPBS. RAI is accredited by the NAPBS and is a member of the Better Business Bureau and Council of International Investigators. You can contact Kevin at [kprendergast@raiglobal.com](mailto:kprendergast@raiglobal.com).







# **INFORMATION SECURITY A TOP PRIORITY FOR BACKGROUND SCREENING FIRMS DUE TO RECENT DATA BREACHES**

*By Dawn Standerwick, Vice President Strategic Growth of Employment Screening Resources (ESR)*

Several widespread and well-publicized data breaches in recent months have made information security a top priority for background screening firms in today's digital age. As a result, background check firms that deal with Personally Identifiable Information (PII) of consumers must be on constant guard against unwanted data breaches and embarrassing cases of identity theft that can affect millions of people.

Information security and data breaches have become big news and big business. Information protection is a critical concern for any business hoping to prevent embarrassing and costly data breaches that can harm a company's reputation and bottom line. The following cases of recent data breaches are just a few examples among many of why businesses need to protect their data from unwanted visitors.

In March 2016, Home Depot Inc. agreed to pay a total \$19.5 million – \$13 million to settle class action lawsuits and \$6.5 million for identity protection services – to compensate approximately 50 million consumers affected by a massive data breach in 2014. Home Depot also agreed to improve information security and hire a Chief Information Security Officer (CISO) as part of the settlement agreement.

In September 2015, credit reporting agency Experian discovered a data breach where an unauthorized party accessed records containing information of T-Mobile users that included names, addresses, dates of birth, and Social Security numbers (SSNs). Experian notified appropriate federal and international law enforcement agencies and took additional security steps to prevent future data breaches.

Also in September 2015, Sony Pictures Entertainment reached a settlement to end class action lawsuits resulting from a data breach hack first revealed in November 2014 that exposed the personal information of thousands of Sony employees online. The lawsuit claimed Sony Pictures did not take adequate measures to prevent the incident that compromised the personal information of thousands.

Even the United States government is not immune to suffering an embarrassing data breach. In July 2015, the U.S. Office of Personnel Management (OPM) announced that information including Social Security Numbers (SSNs) for 21.5 million people were compromised in a data breach involving the background checks of current, former, and prospective Federal employees and contractors.

The issue of information security also rose to prominence on the international stage. In March 2016, the European Union (EU) Commission and the United States (US) agreed on a new transatlantic data transfer framework called the EU-US Privacy Shield that reflects the requirements set by the October 6, 2015 ruling by the European Court of Justice that declared the previous Safe Harbor framework invalid.

The EU-US Privacy Shield places more obligations on U.S. companies that handle the personal data of Europeans to protect that data and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC) that includes robust enforcement, clear safeguards and transparency, and effective protection of EU citizens' rights with several redress possibilities.

So how does a screening firm protect the information of consumers used for background check reports from embarrassing data breaches? A background screening firm, such as Employment Screening Resources® (ESR), that has achieved accreditation by the National Association of Professional Background Screeners (NAPBS) has safeguards in place against unauthorized users and unwanted intrusions.

Since its inception, the NAPBS believed there is a strong need for a singular cohesive industry standard and so created the Background Screening Agency Accreditation Program (BSAAP). Governed by strict requirements and measurements, the BSAAP is an industry "seal" representing a screening firm's commitment to excellence, accountability, high professional standards, and institutional improvement.

To become accredited, a Consumer Reporting Agency (CRA) must pass a rigorous onsite audit, conducted by an independent auditing firm, of its policies and procedures as they relate to six critical areas of the Background Screening Agency Accreditation Program (BSAAP): Consumer/Data Protection; Legal Compliance; Client Education; Product Standards; Service Standards; and Business Practices.

The cornerstone of NAPBS Accreditation is 'Clause 1.1 Information Security Policy' which states CRAs shall have a Written Information Security Policy (WISP) to protect consumer information from internal and external unauthorized access and cover issues such as acceptable use, intrusion detection, data retention/destruction, information sensitivity, passwords, user access, and physical security.

Founded in 2003 as a non-profit trade association, the NAPBS represents the interests of more than 800 member companies around the world that offer background screening. Approximately 10 percent of NAPBS member screening organizations are accredited. A copy of the NAPBS Accreditation standard, the policies and procedures, and measurements is available at [www.napbs.com/accreditation/](http://www.napbs.com/accreditation/).

To add an additional layer of information security, a background screening firm may, like ESR, undergo yearly SSAE 16 SOC (Service Organization Control) 2® Type 2 audit to ensure that the company meets the high standards of the American Institute of Certified Public Accountants (AICPA) to protect the privacy, security, and confidentiality of consumer data used for background checks. Annual SOC2 audits demonstrate a greater commitment to data protection particularly for industries with heightened data protection concerns such as banking and insurance.

SOC 2® audit reports are becoming increasingly important to businesses seeking assurance about the effectiveness of controls surrounding security, confidentiality, and privacy of the systems and information used by screening companies to process the background check orders of their clients. Definitive assurance is only provided through an independent SOC 2® audit report.

ESR's SOC 2® report demonstrates competency in protecting confidential and personal information of clients and their employees from unauthorized access and use. This growing concern in today's digital world needs to be addressed head-on. ESR is committed to protecting any and all information used in the company's background screening services. To learn more, visit [www.esrcheck.com/SOC-2/](http://www.esrcheck.com/SOC-2/).

---

## About The Author



Dawn Standerwick is Employment Screening Resources' (ESR) Vice President Strategic Growth. She has more than 25 years of experience in workforce screening solutions with extensive knowledge of background screening, substance abuse testing and occupational health testing. She currently serves on the executive board as chair elect. She is actively involved on the NAPBS government relations committee and participates in legislative advocacy efforts on behalf of the association.

ESR is a strategic choice. We believe companies deserve a background screening partner they can rely upon to consistently deliver fast, accurate, affordable and compliant information through an innovative, highly-integrated solution that supports employer compliance to comply with ever-changing laws.

ESR is both accredited by the NAPBS and is audited yearly for SOC 2® compliance, a distinction held by a small percentage of background screening firms. Learn more about ESR at [www.esrcheck.com](http://www.esrcheck.com).



# **The Dawning of a New Era in Background Screening!**

**The Background  
Screening Information  
Source You have been  
looking for is here!**

**A Comprehensive Open Source of information for Human Resources and Hiring Professionals. An unmatched Knowledge Center with an extensive Article Library including the top minds in background screening.**



## **PREEMPLOYMENTDIRECTORY.COM**

**"The Information Portal for Background Screening"**



# Discover A New Level of Screening Performance

No Data  
Scraping

Completely Domestic Customer  
Service and Operations Center

No Offshoring of PII



Information  
Security



Quality  
Management



Founding  
Member

There is no other global screening company that takes information security, legal compliance and quality management as seriously as EBI.

Background Screening. Drug Testing. Occupational Health Screening. E-Verify.



Employment Background Investigations • [www.ebiinc.com](http://www.ebiinc.com) • 800.324.7700

Screening News Network<sup>SM</sup>

Bringing You the Latest Screening News and Legislative Issues.

[www.ebiinc.com/screening-news-network](http://www.ebiinc.com/screening-news-network)



EBI is a registered trademark of Employment Background Investigations, Inc.