WHITE PAPER

KEY CONSIDERATIONS FOR SELECTING THE RIGHT BACKGROUND SCREENING PARTNER

Cisive | eVERIFILE a Cisive company | IntelliCorp a Cisive company | Driver iQ a Cisive company | InQuiries Screening a Cisive company | PreCheck a Cisive company | CARCO a Cisive company

How does a company select a background screening service provider? It used to be that a company would call upon subject matter experts who were tasked with the job of finding and vetting quality providers.

Today, as companies seek to constrain costs, the subject matter expert is typically relegated to providing a list of RFP questions to be presented by procurement departments who will make the first cut of respondents. Often, the procurement department will make the initial evaluation of RFP results on cost alone and allow only the lowest cost providers to be submitted to the stakeholders for consideration.

Those who charge more to perform the research in a responsible manner may be eliminated without further consideration. The unintended consequence of putting price before subject matter expertise is that quality and applicant experience most often suffers. Knowing that, many background screening providers therefore take shortcuts, driven by a market that is now focused almost exclusively on cost. These shortcuts have resulted in a large and growing body of litigation alleging violations against both employers and their background screening providers. This paper will further explore how to evaluate a background screening provider and surveys litigation trends while offering guidance to avoid litigation traps.

LITIGATION LANDSCAPE

In today's landscape, many of the lawsuits relating to background checks focus on the Fair Credit Reporting Act (FCRA [15 U.S.C. § 1681 et seq]). The FCRA is the controlling federal legislation for background screening providers when providing background screening reports to employers. When performing background checks under the FCRA, a background screening provider is considered a consumer reporting agency (CRA). Employers or entities that order and use background checks are referred to as end-users of consumer reports and have specific responsibilities under the law.

Within the FCRA, there are two key provisions dealing with accuracy of information: Section §1681e(b) requires that CRAs follow reasonable procedures to assure maximum accuracy of information, and section 1681k(a)(2) requires that CRA assure information is complete and up to date at the time it is reported. The vast majority of cases in which the CRAs alone or the CRA and employer are named parties, include allegations regarding the lack of quality reporting. That fact by itself is highly suggestive of the impact of the low cost segment of the industry.

In addition to sections within the FCRA relating to accuracy that may lead to law-suits, there are various sections requiring consumer notifications. Often, as is the case with the background check disclosure form, notice of investigative consumer report, the pre-adverse and adverse letters, the timing of the notices are specifically prescribed, as well as the general content and presentation; however, the specific wording is left to the end-user. In the case of the Summary of Rights, the timing, actual wording, and even font size are specified and required. Further, CRAs are required under the FCRA to educate end users of their responsibilities under the law and to obtain written certification that they will comply. A background screening partner must be knowledgeable of the various responsibilities outlined within the FCRA to help guide end-users. While end-users are ultimately legally responsible, an informed partner with the proper FCRA certifications and expertise is an invaluable resource to employers.

RED FLAG PRACTICES

Unrealistic Turnaround Time

When comparing background companies, it is easy to consider background screening a commodity because all reports are derived from public sources. In a true commodity market, quality is a given, and only factors like price, delivery, or turnaround time are considered relevant distinguishing characteristics. The truth is that raw data only becomes actionable information when it is properly sourced, verified, and filtered. There are no free lunches. If one or more prospective background providers are offering turnaround times and pricing that appear to be far better than others; that may suggest dangerous shortcuts, such as the use of raw database searches or unverified reports. These are precisely the shortcuts that drag both the provider and the employer into court on allegations of FCRA violations. Significantly lower numbers on package pricing may indicate that either the lead frequency assumptions were under recognized to achieve an artificially low bid, which will balloon in practice after an award is made, or is indicative of habitually careless research that intentionally fails to include all appropriate name, date of birth and/or address combinations exposing the employer to unanticipated risk.

Over Reliance on a 'National' Criminal Database

There is no such commercially available product as a true national database. While the use of compiled criminal databases is a recommended supplemental practice to cover a wider scope since most state courts are accessed only on a county level, there are huge and significant portions of the country that are not covered by these datasets. Even when used properly as a supplemental criminal source, the results need to be verified with research conducted at the appropriate court as the data is often incomplete, outdated, and lacking sufficient identifiers for a positive match. Unfortunately, there are background companies who will provide these databases as standalone searches; either because they fail to educate their clients as to the shortcomings, or to appease employers who think they only need cheap, quick, and easy. Over reliance on compiled databases is another quick route to a poor candidate experience and civil action.

Disclaimers

Background providers should stand behind their work. Period. Any company that includes disclaimers about accuracy or completeness on their reports or in their service agreements is informing the employer that they can expect to be sued over their reports, and that the background provider is expressly not standing behind the quality of their work. Ask for sample reports and service agreements to examine to avoid poor quality work hiding behind disclaimers. Caveat emptor!

Absence of Regular Consultative Engagement

In evaluating prospective background providers, be sure to review RFP or bid response materials for evidence of a true consultative partnership. In the pre-award phase, perhaps the clearest indication of the correct approach is the inclusion of a proposed plan to hold regular and frequent program reviews with the employer. While the preferred frequency may shift over time, with very frequent meetings during and immediately after program implementation to perhaps monthly or quarterly business review meetings for established programs, these meetings ensure thoughtful two-way discussions of the program address not only tactical issues that may arise, but also more strategic and consultative opportunities to improve the candidate or employer experience with the program as well as evolving compliance requirements.

Off-Shoring

Off-shoring is a potential red flag because it is the first indication that the background provider is motivated by low cost over quality and customer service. The only reason to off-shore, is to lower cost. Quality is not a driving factor and, in fact, part of the offshoring decision equation is how to compensate for all the potential pitfalls of offshoring: distance and time-zone differences, turnover, lack of loyalty caused by low wages and competing interests offering pennies per hour more, and physical and cyber security issues. In today's litigious environment and with increasing cyber threats, the loss of data and control over personally identifiable information (PII) is a paramount concern for businesses. Off-shoring increases those risks for very little return.

Having explored red flags, let's take a look at the positive attributes that should be examined.

ESTABLISHING CRITERIA

Accreditation

The Professional Background Screening Association (PBSA) offers an Accreditation program to background companies in which, much like ISO standards, the company develops and documents their policies and procedures relating to Data Information and Security, Legal Compliance, Client Education, Researcher and Data Standards, Verification Service Standards, and Miscellaneous Business Practices. The submitted policies and procedures are first reviewed in a desk audit and then by an onsite review by an independent auditor who makes an accreditation recommendation to the Background Screening Credentialing Council of the PBSA. Accreditation should be considered a minimum selection criterion; especially considering the risks of litigation as described above. There are a sufficient number of accredited background companies, that no employer should risk accepting services from a company that cannot or will not achieve Accreditation.

Key Personnel

Experienced staff with wide ranging and deep skill set can make the difference between success and failure of a company... and a background partnership. Look for a company whose key personnel are active in professional associations and are not only experienced, but have complementary skills including knowledge of the industry, applicable local, state and federal law, compliance, systems and system integration, process improvement, customer and candidate service, and human resource issues.

System Capabilities

The background industry is not just about data; it is also about creating actionable information from raw data, robust communications, and information delivery. Most background providers' systems fall into one of two categories: 1) Licensed software obtained from a platform provider; or 2) Cobbled together systems that have evolved over time and acquisition.

- Licensed software is limited to capabilities in the original design and that which might be supported by the community of users, often resulting in workarounds and compromises.

- Cobbled together systems are the disjointed result of acquisitions never truly delivering robust, unified, and global resources to either the provider or its clients.

When evaluating prospective background providers' systems, you should look for proprietary systems in which the background provider has committed investment and the ability to integrate with your existing systems. Determine whether the provider's system is built on a true rules-based workflow engine that is capable of creating a secure, paperless process and presents an easy to follow workflow for both your candidates and your staff. To avoid becoming a litigation target, you should ensure that the systems, workflows, and processes employed by your provider assist in maintaining compliance with the ever changing legal environment.

Regular Consultative Engagement

In evaluating prospective background providers, be sure to review RFP or bid response materials for evidence of a true consultative partnership. In the pre-award phase, perhaps the clearest indication of the correct approach is the inclusion of a proposed plan to hold regular and frequent program reviews with the employer. While the preferred frequency may shift over time, with very frequent meetings during and immediately after program implementation to perhaps monthly or quarterly business review meetings for established programs, these meetings ensure thoughtful two-way discussions of the program address not only tactical issues that may arise, but also more strategic and consultative opportunities to improve the candidate or employer experience with the program. As the laws evolve, both statutory and those driven by case law, these discussions can address those changes to adjust the program accordingly.

Litigation History

It has been said that the best predictor of future behavior is past behavior. In evaluating prospective background providers, ask if they have ever been the subject of an FCRA violation investigation by the federal regulator, The Federal Trade Commission (FTC), or the Consumer Financial Protection Bureau (CFPB). Ask if they or any company acquired by them, have ever been or is now involved in litigation regarding an alleged FCRA violation. Once you have the facts, you can determine if you would be at risk with that provider or be best served by a background screening provider with a better record.

Client and Candidate Facing Resources

Simply stated, a background screening partner should make your job (and your candidate's job) easier and provide the tools necessary to help you assess further opportunities to improve. These resources include quality, actionable information, the systems mentioned above, standard, custom and ad hoc reporting, and, most importantly, the consultative partnership to help you achieve your goals. In evaluating prospective providers, ask to see sample reports, both individual and management reports. Ask to see the online resources available both to the line management administering your program internally and to your candidates. Establish hours of service, not only to your staff, but to your candidates. You should insist on a 24 x7 help desk because most of your candidates will be filling in applications and forms after hours. Determine if the prospective provider has the ability to efficiently reach out to candidates when clarification is needed and if they have the ability to track and manage that outreach. Ask if the provider has the ability to benchmark and if they are willing to host roundtable events including other clients similar to you to explore ways to make your programs more effective, or to deal with changing legal or regulatory issues.

Data Security

Data security and protection of your candidates' and employees' PII has never been more challenging and more critical than it is today. This topic needs a white paper all by itself, but there are basic questions that should be asked.

- Does the provider have a data security (and business continuity) plan? Part of that plan should include regular intrusion testing by an independent company and a code review to look for and repair vulnerabilities. Data should not only be encrypted when accessed remotely, but should be encrypted at rest.
- Evaluate the physical security of the network. Who has access? Is it private and proprietary, or does the provider share

the servers of a public host who may serve multiple background companies licensing their software?

- Is the processing and/or network storage in the U.S. or perhaps in a less secure environment? Compare how data is backed up, and what the latency of that backup is. You should compare how quickly service could be restored in the event of a catastrophic failure of the main storage site. Question the password policy and how frequently passwords are expired. Internal threats to data security are often overlooked.
- Be sure to evaluate the prospective background providers own background policy and whether they have an effective internal security awareness training program for their own staff to guard against data theft through carelessness or social engineering. It is recommended that you visit at least the primary processing and network storage facilities to perform an onsite assessment if possible.

Research Philosophy

This topic was covered in the Red Flags section, but to review, the background provider you select should be willing to stand behind the report they deliver. To do that, the background provider should perform original, contemporaneous research at original source providers and verify that the information to be reported is relevant, accurate, up to date, and legally compliant when it is reported. Question how databases might be used and question that use if reports are generated from unverified databases. Many courts offer remote online access to index information that is often incomplete. While it is sensible to take advantage of these indices for preliminary research, question the extent to which information from online sources is validated or verified. Do not accept "name match only" results or incomplete records. The same position holds true for employment or education verifications. It is possible that an initial adverse result might be obtained from a source clerk who was rushed, careless or unaware of supplement records. Ensuring that adverse results are re-verified reduces exposure to claims of unfair hiring practices due to reliance on faulty background reports, and preserves good candidates, thereby shortening hiring cycles!

Selecting a background screening provider is not a simple task, and the stakes are high. There is risk to the company and its employees and shareholders if the background screening program is deficient. It should not be assumed when reviewing pricing proposed in response to an RFP that you are seeing a true "apples to apples" comparison. The quality of background services varies widely and, as the brief litigation summary at the beginning of this white paper suggests, quality does matter. The wrong decision can be very costly both in monetary terms and in reputational damage. Understand the red flags. Be prepared to evaluate quality and organizational fit to assess the long term cost of your relationship with a background screening provider. Those who persist in chasing pennies in the selection phase will be feeding dollars to litigation and lawsuits in the future.

ABOUT CISIVE

Cisive, headquartered in Holtsville, New York, is a leading background screening provider focused on providing high-value employment background checks and industry-specific compliance services to highly regulated, risk-sensitive industries. Cisive has long-term relationships with a diverse base of clients across healthcare, financial services, transportation and other regulated industries.

Founded in 1977, Cisive has developed a broad range of differentiated vertical business lines and risk mitigation offerings including the core Cisive brand (global and enterprise), PreCheck (healthcare), Driver iQ (trucking and transportation), eVerifile (rail and contractor), Inquiries Screening (government), IntelliCorp (small and mid-market) and CARCO (insurance risk mitigation). Cisive's solutions deliver compliant employment intelligence to employers who are highly averse to employee-related risks and operate in highly regulated industries.

With Cisive, your business will not only gain a background screening provider, but a true partnership: a company that stands by our work, protects our clients, and provides the consultation and guidance world-class organizations seek.

CONTACT US

www.cisive.com

info@cisive.com

866.557.5984

Cisive | eVERIFILE | IntelliCorp | Driver iQ | InQuiries Screening | PreCheck | CARCO