THE INCREASING DANGER OF BACKGROUND CHECKS: NEW LAWS AND EMERGING PRIVACY RIGHTS COMPLICATE AN ALREADY DIFFICULT PROCESS

08.25.2015
Employment Law Reporter, Ervin Cohen & Jessup LLP

PROFESSIONALS

Kelly O. Scott

PRACTICE AREAS

Employment

The intersection of privacy laws and employment practices can be a dangerous one. Employers who perform background checks on applicants must navigate through multiple state and federal data privacy laws, information security statutes, regulations and, of course, employment laws, each of which governs aspects of the hiring process.

Credit Reports and Histories

The Society for Human Resource Management reports that approximately one-half of all employers use credit checks in the job application process. Many argue that the use of credit reports in this manner is unfair, that credit reports are more likely to reflect family economic hardship than a lack of judgment, and that they simply are not relevant to the qualifications required for the majority of positions for which they are used. As a result of these arguments, a growing list of states, including Hawaii,[1] Illinois,[2] Oregon,[3] California, Vermont, Nevada, Connecticut, Maryland, Washington and Colorado, restrict companies from making employment decisions based on an applicant's credit report or other credit history except under limited circumstances. However, even where companies may use such information in hiring decisions, the Fair Credit Reporting Act ("FCRA") requires employers to provide applicants with a copy of their credit report, as well as a written description of their rights under FCRA, so applicants have an opportunity to correct any inaccuracies before the prospective employer makes any decisions based on the information.[4]

Criminal Background Checks

Over the last several years the Equal Employment Opportunity Commission ("EEOC") has sought to limit employer inquiries regarding criminal records based on a growing concern that hiring policies that screen out those with

past criminal records can disproportionately preclude African Americans and Hispanics from employment opportunities. The concern is based on the fact that national data shows that African Americans and Hispanics are arrested and incarcerated at rates disproportionate to their numbers in the general population. Accordingly, in 2012, the EEOC issued an Enforcement Guidance that recommends that employers should altogether eliminate policies or practices that exclude individuals from employment based on any criminal record, and to ensure that all managers, hiring officials, and decision makers are trained about Title VII and its prohibition on employment discrimination.

The movement to "ban the box" and give applicants a fair chance to be judged based on their qualifications rather than their past mistakes has caught fire: over 100 cities and counties and 18 states have passed laws eliminating the criminal conviction question from the job application process and delaying criminal background checks or questions until the applicant has been determined to meet the initial qualifications for the position.

When permitted, companies performing criminal background checks must also be wary of seeking too much information, or improperly using such information, once obtained. The FCRA only permits consumer reporting agencies to report on convictions for up to seven years. Moreover, California, Colorado, Kansas, Maryland, Montana, Nevada, New Hampshire, New Mexico, New York, Washington and Massachusetts all have laws limiting inquiries by employers into criminal convictions. These laws generally prevent employers from making inquiries regarding convictions that are more than seven years old. Other restrictions related to specific types of convictions, such as those relating to sealed or expunged convictions, or juvenile convictions. For example, California is one of several states that prohibits the use in employment decision-making, of sex offender information obtained from the State's "Megan's Law" website, unless it is used to protect a person at risk.[5] Improper use will subject employers to liability for actual damages, punitive damages, attorney's fees and civil penalties of up to $25,000.[6]

Storage, Security & Disposal of Information

In addition to all of the rules pertaining to the procuring and use of credit and criminal background checks, employers must take care to properly safeguard and dispose of the information collected. Employers who obtain background checks on candidates should properly dispose of all such information as soon as possible. Federal law, specifically the Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule requires: ". . . any person who maintains or otherwise possesses consumer information for a business purpose" to properly dispose of such information.[7]

If employers have a need to keep such information, such as in accordance with law requiring the employer to keep certain information actually used in employment decisions, both FACTA and state privacy laws require them to protect this data from unauthorized access or use. For example, California requires that "a business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect that information from unauthorized access, destruction, use, modification, or disclosure."[8]

New Technologies, Same Principles

Some employers use (or are) third-party vendors that provide background information used in the pre-employment process. The Federal Trade Commission has made it clear that this information constitutes "consumer reports" under FCRA: "when companies provide information to employers regarding current or prospective employees' criminal histories, they are providing "consumer reports" because the data involves the individuals' characters, general reputation or personal characteristics."[9] This is true even when the employer uses a mobile app to obtain or process the information. Employers must also be circumspect when seeking social media information on candidates. About half of states, including California, prohibit employers from forcing applicants to disclose passwords for social media sites such as Twitter or Facebook, to allow the employer to view their profile. Indeed, even where an employer (or its agent) reviews an applicant's public posting (or "blog") with multiple postings by a candidate, it must take care not to allow the person making the hiring decision to become aware of the candidate's political or religious views, or similarly "off-limits" information that could improperly taint a hiring decision. For this reason, some employers use a third-party service to scan social media sites, or separate these functions within the company.

Digital technologies have both improved and complicated the pre-employment screening process. Employers would do well to heed the warnings of the FTC, EEOC and other watchdogs that seek to safeguard the privacy and personal information of candidates. Employers should therefore consider if such information is genuinely relevant to the qualifications for the position and, if so, take steps to ensure that the information sought is obtained, used, maintained and discarded in accordance with applicable federal, state and local laws.

[1] See H.R.S. § 378-2(a)(8).

[2] See 820 ILCS 70/10.

[3] See O.R.S. § 659A.320.

[4] See 15 U.S.C.A. §§ 1681 (a) – (u).

[5] See Cal. Penal Code §290.46(1).

[6] See Cal. Penal Code §290.46(1)(4)(A).

[7] 16 C.F.R. Part 682; see also Cal. Civil Code §1798.81.5 (requiring personally identifying information to be disposed of "properly" . . . "to make it unreadable by any means . . .").

[8] Cal. Civil Code § 1798.81.5(b).

[9] Federal Trade Commission to Everify, Inc., Jan. 25, 2012, available here.