Are You Carefully Vetting Your Third Party Vendors? If Not, You May Be Buying Yourself a Breach of Privacy Claim

Insights
9.10.18

Our client, we'll call them **Company X**, provides installation, connection, upgrades and repairs for one of the country's largest providers of residential and commercial television, telephone and Internet service. We'll call their customer **Company Y**. Pursuant to their contractual agreement, our client (Company X) retained a third party vendor to conduct civil and criminal background checks on job applicants. However, in the last year **Company Y** was purchased by **Company Z,** an even larger provider of television, telephone and Internet services. **Company Z *requires*** our client to utilize a different third-party vendor for conducting background checks.

Rather than follow guidelines from the U.S. Equal Employment Opportunity Commission, which recommend limits on the temporal scope of background checks – five years – the new provider looks back through the working lifetime of the applicants. Also contrary to EEOC guidelines, the new provider considers juvenile offenses and non-convictions in determining whether an applicant is a suitable job candidate. **Company Z** obliged our client to utilize the new provider for background checks, and required new background checks be conducted on the current work force. When the new background checks found charges or convictions on current employees, no matter how old the charges or the age of the worker at the time of the offense, they denied the workers permission to continue working for our client. Several workers suffered real harm as a result – job loss. In turn, the terminations generated a threatened lawsuit by a fired current employee, for violation of the Fair Credit Reporting Act and for invasion of privacy. In one case, the criminal charge occurred more than seventeen (17) years ago, when the worker was a juvenile. Attorneys for the fired employee threatened suit on the worker's behalf, and threatened a collective action lawsuit on behalf of all similarly situated workers. The claim ultimately settled, before it became an expensive, time consuming, and distracting collective action.

This is of course an unusual circumstance, in which our client did not have the opportunity to vet the third-party vendor who eventually placed them in the unenviable position of defending an invasion of privacy lawsuit. However, it points up real reasons why all employers need to closely examine the credentials and background (if you will) of their third-party vendor who will be providing background check services. Frankly, any third-party vendor who will gain access to an employer's employee or job applicant information should be reviewed thoroughly ahead of entering any contractual or working relationship. This is important because this area of employment practices – background checks and resulting invasions of privacy --is a prime source of litigation for plaintiffs

and the plaintiff's bar. Some questions to ask include what are the vendor's regular practices? What steps do they take to protect employee or applicant information you provide? Are their forms accurate in disclosing rights and information under the FCRA? Are their disclosures to applicants and current employees appropriate? Have they been sued previously for FCRA or other privacy breaches?[1]

To be sure, some case law has provided some protection for employers. In March 2017, in the matter of *Dilday v. Direct TV,* the U.S. District Court for the Eastern District of Virginia found that a technical violation of the FCRA was not actionable by a single plaintiff under the Fair Credit Reporting Act because the plaintiff did not suffer any real harm, or an "injury in fact", and therefore could not show his privacy had been invaded. Real harm, or an "injury in fact", would have been the key issue in our client's case, had it not been resolved. Interestingly, the decision in *Dilday v. Direct TV* contradicted a different result by a different judge in the same court, the Eastern District of Virginia. In the matter of *Thomas v. FTS USA,* the court found that the FCRA generally did confer "a right to privacy of one's own personal information." It is expected that this conflict between two district courts, which are on appeal, may find their way to the U.S. Supreme Court for resolution.

[1] As our colleague, Brian Ellixson, Esq. pointed out in this space a week ago, employers should also review their agreements with vendors for indemnification clauses, limitations on liability and language on who pays in the event of a privacy breach.

Related People

Andrew Froman
Partner
813.769.7505
Email

Service Focus

FCRA and Background Screening