Published on *The National Law Review* https://natlawreview.com

CFPB Issues Guidance With Aggressive Interpretation of FCRA Applicability to Employee Monitoring and Screening Tools

Article By:

Benjamin W. Perry

Gustavo A. Suarez

Lauren N. Watson

The Consumer Financial Protection Bureau (CFPB) recently issued guidance that takes an aggressive position regarding the scope of the Fair Credit Reporting Act (FCRA) as covering certain employee monitoring and assessment tools used for hiring and to gauge employee productivity. This development affects virtually every employer using third-party vendors for employee screening, monitoring, or assessment.

Quick Hits

- The CFPB's recently issued guidance on the Fair Credit Reporting Act affects virtually every employer using third-party vendors for employee screening, monitoring, or assessment.
- The guidance serves as a reminder for employers that gather third-party information to vet job applicants to consider whether their third-party vendors' practices trigger FCRA requirements.
- This guidance also highlights ongoing regulatory trends toward increased scrutiny of workplace monitoring and AI-powered assessment tools.

What Makes a Tool Subject to the FCRA?

The CFPB provides a (facially) straightforward framework to determine if a company's vendor relationships trigger FCRA obligations. The key questions are whether the tool is used for employment purposes (including hiring, promotion, reassignment, or retention) and whether the vendor assembles or evaluates consumer information to produce reports.

Importantly, companies developing AI algorithms may qualify as consumer reporting agencies if they collect data from multiple sources to train their algorithms or generate worker assessments. This means that many popular workforce analytics platforms and AI-powered hiring tools could fall under the FCRA's purview if they are combining employee or job applicant information with information

derived from other sources. In today's environment, where many artificial intelligence tools are a "black box" in terms of the information on which they've been trained, this analysis will likely prove especially tricky.

Navigating the FCRA in an AI- and Data-Driven Landscape

The traditional understanding of the FCRA's scope in employment—largely limited to background checks and credit reports—is consistent with some portions of the CFPB's guidance, while other portions of the guidance represent new compliance challenges for employers to navigate. In Circular 2024-06, the CFPB states: "Similar to credit reports and credit scores used by lenders to make lending decisions, background dossiers—such as those that convey scores about workers—that are obtained from third parties and used by employers to make hiring, promotion, reassignment, or retention decisions are often governed by the FCRA."

This interpretation is not a novel take or an interpretive expansion of existing FCRA applicability. Instead, it serves as an important reminder for employers that gather third-party information to vet job applicants to consider whether their third-party vendor providers trigger the FCRA requirements. With the rise in reports of applicants using false identities to infiltrate company networks and install malware, steal sensitive company data, or funnel earnings to sanctioned countries like North Korea, ensuring compliance with the FCRA when using such background information is more critical than ever, as employers are increasingly turning to nontraditional applicant vetting companies to root out fake applicants.

This is where the CFPB guidance's traditional and commonsense understanding of the FCRA's scope ends. The CFPB next opines that other tools, such as those that monitor employee driving and generating an algorithmic score, could also be subject to the FCRA's requirements. Under the FCRA, a third-party tool or company can qualify as a "consumer reporting agency" (CRA) if it "assembles" or "evaluates" consumer information and generates reports used for employment decisions. Notably, the FCRA applies to tools that gather or assess information about a worker from external or third-party sources but *not* to reports generated based solely on interactions and transactions between a consumer and the entity making the report. Here's how this requirement plays out in different scenarios:

- **Using third-party data:** Suppose a scoring tool generates assessments by combining an employee's work performance with data from public records, other employers, or commercial databases (like data on unionizing activity or financial stability). This practice can turn the tool into a "consumer reporting agency," as it assembles or evaluates information collected from multiple sources to deliver a report that would be used for employment decisions.
- **Aggregating cross-employer data:** Some companies collect information from several employers, such as past performance metrics, disciplinary history, or even driving records if the employee worked in different locations or roles requiring driving. When these historical details from various employers are evaluated to generate a risk or productivity score, the company assembling this information could be deemed a CRA because it is creating a comprehensive report that impacts employment.
- **Leveraging public and commercial data for scoring:** A tool that combines an employee's productivity score with public data (e.g., criminal records and bankruptcy filings) or demographic information can also cross into FCRA territory. These sources of data are traditionally considered consumer report information under the FCRA. When blended with an individual's internal employment data to create a more holistic score, the FCRA would likely classify this as a consumer report.

- **Algorithmic models trained on third-party data:** Even if a tool is not directly aggregating other sources for each report, a model trained on third-party data might still be in FCRA territory if the algorithm produces scores based on patterns it identified from a broader set of consumer information. For instance, if an app tracking driving behavior also factors in national or regional data on similar worker profiles, this might involve “assembling” consumer information as defined by the FCRA, according to the CFPB’s interpretation.
- **Consumer data not related to employer transactions:** The FCRA has an exemption for data reflecting “transactions or experiences” between the worker and his or her employer only. However, if a report includes data from outside this relationship—such as external sources, past employers, or even aggregate industry benchmarks—the CFPB is taking the position that this would generally fall outside the scope of this exemption. The inclusion of nontransactional, consumer-related data makes the report subject to FCRA requirements, according to the CFPB.

In recent years, companies have begun to rely on algorithmically generated scores to monitor worker productivity, assess risk, or predict behavior. Examples include monitoring driving habits, tracking computer use, and assessing productivity. Under this expansive interpretation by the CFPB, these scores may be categorized as consumer reports if they impact employment decisions and are compiled by a CRA.

Critical Compliance Requirements

Under the FCRA, employers must provide a disclosure and obtain an individual’s consent before procuring reports. Likewise, they must undertake a specific pre-adverse and adverse action process before taking adverse action. This applies not just to initial hiring decisions but to ongoing employment actions like promotions, reassignments, or terminations. Employers generally must fulfill several key obligations when using consumer reports for hiring or other employment-related decisions:

- **Provide disclosures and obtain authorization:** Before procuring a consumer report, employers must provide federal, state, and local disclosures and obtain separate, written authorization from the applicant/employee. This ensures transparency and gives workers an opportunity to understand what information will be used in their evaluation.
- **Provide a pre-adverse action letter:** If an employer is considering taking adverse action (such as denying a promotion or terminating employment) based, in whole or in part, on the consumer report, it must provide a pre-adverse action letter, with appropriate federal, state, and local notices, along with a copy of the report. This allows the individual an opportunity to dispute inaccuracies or provide additional information or context.
- **Wait a reasonable period of time:** An employer must wait a minimum of five business days after the applicant/employee receives the pre-adverse action letter. Some jurisdictions may require a longer period.
- **Notify workers of an adverse action:** Upon making an adverse decision, the employer must notify the worker of the action, provide contact information for the consumer reporting agency, and inform the worker of their right to dispute the report’s content, along with other applicable federal, state, or local disclosures.
- **Restrict use of reports to permissible purposes:** Employers may only use consumer reports for purposes allowed under the FCRA, which include evaluating a candidate’s suitability for hiring, promotion, reassignment, or retention.

Please note that certain jurisdictions may require additional/different processes.

Business Impact and Next Steps

Companies may want to evaluate several steps to balance their legitimate need for workforce monitoring against these expanded compliance requirements. The first step is a thorough review of HR technology stack and vendor relationships, with a particular focus on tools that make or inform employment decisions—a task that entails developing a compliance framework that addresses both traditional background checks and newer technological solutions. The cost of noncompliance, including potential regulatory enforcement and private litigation, makes this a priority for risk management.

Looking Forward

This guidance signals increased regulatory scrutiny of workplace monitoring and AI-powered assessment tools. Companies that proactively address these requirements will be better positioned to manage risk while maintaining effective workforce management practices.

National Law Review, Volume XIV, Number 311