

# AI Alert: CFPB Tightens FCRA Rules for Employers

Blythe E. Lovinger, Alison Frimmel, Darby B. Hobbs

November 1, 2024

On October 22, 2024 the Consumer Financial Protection Bureau (CFPB) released the final version of the Personal Financial Data Rights Rule (that we reported about [here](#)). However, the CFPB did not rest there, two days later it also issued a [circular](#) relating to the Fair Credit Reporting Act's (FCRA) application to background reports and algorithmic scores. This policy statement – which reflects the direction in which the CFPB is trending – could have far reaching effects for employers, for which the FCRA has long been a hotbed for class claims and compliance issues, as well as makers of certain software or monitoring tools.

## The Fair Credit Reporting Act and Employer Background Checks

The FCRA is sometimes considered the U.S.'s original privacy statute. Passed in 1970, it provides consumers with the right to access and dispute information in reports created by consumer reporting agencies (CRAs) that are used in making eligibility determinations, including decisions relating to employment.

The FCRA regulates information in the form of “consumer reports,” a term defined by the statute to include “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for” certain purposes including “employment purposes.”

The FCRA imposes specific obligations on CRAs as well as employers using their services to conduct background checks. Background screening reports are a type of consumer report put together by CRAs and provided to employers to help them determine whether to hire, retain, promote, or reassign an individual. As employers well know, when consumer reports such as background checks are used for employment purposes, employees have additional rights and employers are subject to the FCRA’s notice, disclosure and consent requirements.

For example, employers must not only provide employees statutorily-required notice that they intend to obtain a consumer report, but they must also obtain written permission from the job applicant or employee before obtaining any consumer report. In addition, an employer must meet additional notice requirements if it intends to take an adverse action based entirely or in part on a consumer report supplied by a CRA, and this notice obligation arises both *before* and *after* the adverse action.

A boon for workers rights, the FCRA’s many requirements has long presented compliance issues for employers and CRAs.

## The CFPB Circular

As the FCRA's legal complexities evolve, more employers are adopting technology to track workplace productivity and aid in the hiring process. The CFPB's recent circular raises concerns that these tools, provided by CRAs and used by employers, may effectively generate consumer reports, thus necessitating compliance with FCRA regulations.

According to the CFPB, if a tool is provided by a third party that gathers data from public records, employment history, and other relevant information and or uses information beyond the employer's experience with an employee, the tool may be covered by the FCRA. The CFPB states that when assessing whether an employer makes decisions based on a report from a third party regulated by the FCRA, enforcers should focus on two considerations:

- Does the employer's use of data qualify as a use for "employment purposes" under the FCRA?; and
- Is the report obtained from a "consumer reporting agency," meaning that the report-maker "assembled" or "evaluated" consumer information to produce the report?

To illustrate this point, the CFPB cites the example of a phone app that monitors a transportation employee's driving and provides a driving score to the employer for employment purposes. If the app was developed using data from a range of third-party sources, then it could be considered a CRA and the score it assigns to the employee, a consumer report.

For the app maker, this would necessitate compliance with the FCRA and require, among other things, that it have procedures in place to ensure maximum possible accuracy, only provide the app to those with a permissible purpose, and implement a dispute process.

For the employer, this would mean ensuring their own compliance with the FCRA, including by, among other things, providing adverse action notices if they take any action based on the score. To complicate matters, in the driving app example, if employers also provide information that is used to further develop and refine the app scores that are provided to other companies that use the app, the employers could be considered furnishers under the FCRA and would also need to implement a process by which consumers can dispute the accuracy of the information contained in the report.

## Putting Employers on Notice

This circular is putting employers and makers of certain software or monitoring tools alike on notice that the CFPB plans to scrutinize performance and monitoring tools to determine if they fall within the FCRA's ambit. The CFPB is taking a broad approach to what constitutes "assembling" and "evaluating" (key components of the FCRA's definition of a CRA). It will carefully consider tools, especially AI tools, that use large amounts of data for their development and maintenance to determine whether the tool is providing consumer reports rendering the developer a CRA.

The circular also reflects that the CFPB is abandoning a longstanding interpretation that the FCRA does *not* apply to software developers. In 1997, the FTC announced that a company that sells software that allowed the purchaser to compile consumer report information from other CRAs was not itself a CRA because it did not "assemble and evaluate" information itself. The CFPB now says that this interpretation is outdated. The CFPB believes that business models where the software developer licenses software and provides ongoing customer service and maintenance are different in kind from selling software as a "point-in-time product." Taken together, it is clear from the circular

that the CFPB is focused on ensuring the objectives of the FCRA will not be outpaced by technology.

## What Is Next for Employers?

Employers in particular need to take an inventory of the tools that they have implemented to analyze worker data and assess whether they may constitute consumer reports.

Based on the circular, key to these considerations will be whether or not the data is employed for “employment purposes,” and if the tools include or were developed using any data from third parties.

To accomplish this, employers should take steps to understand how the tools they have implemented were developed. This may include reviewing vendor services agreements and require consulting with vendors.

Ultimately, whether a monitoring or performance tool qualifies as a consumer report will depend on a close consideration of the particular facts of its development, maintenance, and use. Employers in particular should consider engaging counsel to audit for any potential compliance concerns.

\*\*\*

Although at this stage the CFPB’s circular raises more questions than it answers, the Kelley Drye team will continue to monitor for any additional guidance, enforcement efforts, or private litigation that sheds light on the breadth of the FCRA’s sweep over these tools.