Employers and Vendors Have FCRA Obligations When Using Workplace AI Tools: Your Step-by-Step Compliance Guide

Insights
11.12.24

The government recently reminded employers and vendors that they have obligations when it comes to use of workplace-related AI tools – and your business may need to update its practices in order to comply. The Consumer Financial Protection Bureau's (CFPB) October 24 Circular reminds employers that their obligations under the federal Fair Credit Reporting Act (FCRA) may extend to employee monitoring, assessment, and AI tools. Given how commonplace such tools are around the country, this Circular will no doubt serve as a wakeup call for many employers across all industries – as well as for the vendors who provide such tools. What do employers and vendors need to know to evaluate the applicability of FCRA to employee monitoring, assessment, and AI tools, and to comply with their obligations under this law?

How the Circular Connects the Dots on Third-Party Technology Vendors as Consumer Reporting Agencies

While there is a tendency to think of background screening companies as synonymous with consumer reporting agencies, FCRA has a broader definition. Broadly speaking, any company that regularly engages in assembling or evaluating information on consumers for the purpose of furnishing consumer reports to third parties falls under this definition.

- A "consumer" is any individual – including job applicants and employees.
- A consumer report, in turn, is any report or other communication by a consumer reporting agency bearing on the consumer's character, reputation, personal characteristics, or more, used, expected to be used, or collected to establish an individual's eligibility for, among other delineated purposes, an employment purpose (although FCRA also applies in many contexts outside of the workplace).

In other words, a company whose business model is to collect employee data vis-à-vis monitoring or screening software or which is provided by employers for AI algorithms may be, at least according to the CFPB's October 24 Circular, a consumer reporting agency.

Under the Circular, if a company uses worker data from employers or public sources to train an algorithm that generates employee scores or assessments, it may also be considered a consumer reporting agency.

The information that such companies provide back to the employer, in turn, may also be a consumer report. Therefore, even though the companies may be working in a closed loop in which they collect information provided by an employer and in turn provide it back to the same employer, that may still be enough to make these technologies vendors a "consumer reporting agency" – and the information provided by them a "consumer report."

Conduct Triggering FCRA Obligations

When obtaining or using a consumer report for an employment purpose, which includes evaluating an individual for employment (*i.e.*, rejecting an applicant or withdrawing a conditional offer), for reassignment or promotion, or for continued employment (*i.e.*, potential discharge), employees need to comply with the FCRA.

But, as articulated by the CFPB's circular, the type of monitoring, assessments, or AI tools which may trigger an employer's obligation to comply with FCRA include:

- Monitoring workers' sales interactions;
- Tracking workers' driving habits;
- Measuring the time that workers take to complete tasks;
- Recording the number of messages workers send and the quantity and duration of meetings they attend;
- Calculating workers' time spent off-task through documenting their web browsing, taking screenshot of computers, and measuring key stroke frequency; and
- Analyzing worker data in order to provide reports containing assessment or scores of worker productivity or risk to employers, including automated recommendations or determinations relating to worker pay, predictions about worker behavior (including potential union organizing activity and likelihood that a worker will leave their job), scheduling shifts or job responsibilities, or issuing warnings or other disciplinary actions.

Employer and Consumer Reporting Agency FCRA Obligations

FCRA imposes various obligations on employers and consumer reporting agencies. Employers must take certain steps before obtaining a consumer report as well as before and when taking an adverse action based on that report. Bear in mind that state laws and local ordinances may impose additional obligations and restrictions.

Before an Employer Obtains a Consumer Report

The employer is required to:

- **Tell the applicant or employee that you might obtain and use information in a consumer report for decisions related to their employment.** This disclosure must be clear and conspicuous, in writing, consist solely of the disclosure, and be a stand-alone document. The disclosure cannot be in an employment application.
- **Get written permission from the applicant or employee.** While this written authorization can be part of the disclosure, it is often itself a separate standalone document. If you want the authorization to allow you to get consumer reports throughout the person's employment, make sure you say so clearly and conspicuously (although such evergreen provisions are not permitted and/or recognized in all states).
- **Certify compliance to the company from which you are getting the applicant or employee's information.** Generally, and in addition to certifying your permissible purpose, you must certify that you:
    - notified the applicant or employee and got their permission to get a consumer report;
    - will comply with the pre-adverse action (and adverse action) notice requirements of FCRA if they become applicable; and
    - will not discriminate against the applicant or employee or otherwise misuse the information, as provided by any applicable federal or state equal opportunity laws or regulations.

Before an Employer Takes an Adverse Action

Before you reject a job application, withdraw a conditional offer, reassign an employee, terminate an employee, deny a promotion, or take any other adverse employment action based on information in a consumer report, you must give the applicant or employee:

- a notice that includes a copy of the consumer report in question; and
- a copy of A Summary of Your Rights Under the Fair Credit Reporting Act, which the company that gave you the report should have given to you – although this document is also available on the CFPB's website.

Providing this "pre-adverse action notice" gives the individual an opportunity to review the report and provide additional information that may be relevant to your decision-making or to challenge the accuracy of the information in the report.

When an Employer Takes an Adverse Action

After providing the pre-adverse action notice, if, after waiting a reasonable period of time, you ultimately decide to take an adverse action based on information in a consumer report, you must give the applicant or employee a notice of that fact – orally, in writing, or electronically. This notice tells people about their rights to see information being reported about them and to correct inaccurate

information. The "adverse action notice" must include:

- the name, address, and phone number of the consumer reporting company that supplied the report;
- a statement that the company that supplied the report did not make the decision to take the unfavorable action and can't give specific reasons for it; and
- a notice of the person's right to dispute the accuracy or completeness of any information the consumer reporting company furnished, and to get an additional free report from the company if the person asks for it within 60 days.

Additional information may be required to be included in this adverse action notice in certain contexts.

Obligations of Consumer Reporting Agencies

The FCRA imposes a myriad of duties on consumer reporting agencies, including:

- Consumer reporting agencies are prohibited from reporting outdated negative information (generally, that would be information that is more than seven years old, or bankruptcies that are more than 10 years old).
- Consumer reporting agencies must respond to file disclosure requests. They must, upon request, disclose the identity of anyone who has obtained the consumer report for employment purposes in the two-years preceding the date the request is made.
- Consumer reporting agencies must maintain reasonable procedures to assure that the information contained in their reports is accurate ("maximum possible accuracy").
- Consumer reporting agencies must conduct reinvestigations into disputes.
- Consumer reporting agencies have an obligation not to share consumer reports absent a FCRA-permissible purpose.
- Consumer reporting agencies must obtain certain certifications from users of consumer reports.

Your Next Steps as an Employer

1. Audit Your Current Practices. Employers should review all third-party employment screening, monitoring, or AI tools to evaluate whether the vendors who provide those tools qualify as "consumer reporting agencies" and whether they generate "consumer reports" under FCRA. Not all monitoring will trigger FCRA requirements. For example, routine monitoring of networks or emails which is meant to capture external bad actors and through which no actions are taken against employees would generally not be covered by FCRA.

2. Understand the Products You Are Using. If vendors cannot explain how they came to the output of any metrics provided, there may be limited utility as well as increased legal risk in using products which cannot clearly articulate how they came to the results they did. Thus, while technology that

tracks driving habits or measure the time spent web browsing may provide concrete and verifiable metrics, assessments used to predict worker behavior or risks to employers may be trickier to validate.

3. Update Your FCRA Compliance Procedures. Employers should review their existing FCRA compliance processes to ensure that they are complying with the requirements imposed by FCRA, including providing disclosures, obtaining authorizations, providing certifications to consumer reporting agencies, and providing pre-adverse and adverse action notices. Employers should proactively identify in what situations pre-adverse and adverse action notices may be necessary given their use of consumer reports for employment purposes.

4. Review Your Vendor Contracts to Understand How They are Using Your Data and For How Long They are Retaining It. While vendors may only use the data they collect from a particular employer for that employer, employers may nevertheless want to confirm that is the case with the vendors they are using. Companies that provide information to consumer reporting agencies have a legal duty to investigate disputed facts. If data you provide is being used outside of an employee's employment with your company, the data may come up in an employee's future employment – and you would have a legal obligation to investigate any disputed facts.

5. Train Your Employees. Managers and HR staff should be trained on the expanded (or, at least, clarified) situations where the FCRA may apply as well as on the FCRA's requirements. Companies may want to consider implementing procedures that funnel all employment actions which may trigger the pre-adverse and adverse action notice process through HR to ensure that proper procedures are followed.

6. Evaluate Whether You May Have Additional Obligations under State Analogs to FCRA. Multiple states have mini-FCRA laws which impose additional obligations. Employers with employees in such states need to evaluate whether those state laws also apply and, if so, ensure compliance with them as well. Similarly, employers should evaluate whether other types of laws, such as EEO laws or state and local Fair Chance provisions, could impact their ability to obtain and/or use consumer reports (and, where applicable, ensure compliance with them as well).

Your Next Steps as a Vendor

1. Evaluate Whether Your Business is a Consumer Reporting Agency. Vendors collecting or analyzing worker data (including AI/algorithm developers using external data to generate worker scores) likely qualify as "consumer reporting agencies." Because FCRA imposes additional obligations on consumer reporting agencies, it is important that vendors evaluate whether they will be subject to such obligations.

2. Understand the Obligations FCRA Imposes on Consumer Reporting Agencies and Develop Corresponding Processes and Procedures to Ensure Compliance. While a full discussion of the various duties imposed by FCRA on consumer reporting agencies is beyond the scope of this article

various duties imposed by FCRA on consumer reporting agencies is beyond the scope of this article, this would include, among other things, developing procedures to address requests to access consumer reports and consumer disputes. Consumers (including employees) have a right to know what is in their file with a consumer reporting agency. Vendors will need to develop processes to handle such requests. Additionally, consumer reporting agencies are required to investigate disputes alleging inaccurate information. Vendors may find themselves needing to work with the employer in order to investigate the accuracy of data. To the extent that vendors use AI to develop metrics, vendors may run into a "black box" problem – if you cannot explain how your algorithm or AI came to a conclusion, you may need to delete the result from the consumer report.

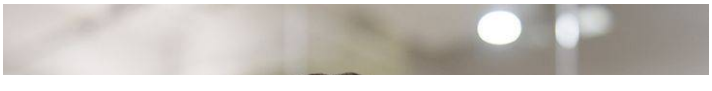
3. Evaluate Whether You May Have Additional Obligations under State Analogs to FCRA. Like for employers, consumer reporting agencies are subject to the state variations on FCRA laws and will need to evaluate their applicability and ensure compliance. Similarly, consumer reporting agencies need to consider whether other laws, including state laws and local ordinances, impose additional obligations on them and their business (and, where applicable, ensure compliance with them as well).

Conclusion

If you need help updating your policies or have questions, contact your Fisher Phillips attorney, the authors of this Insight, any member of our FCRA and Background Screening Group or our AI, Data, and Analytics Team. Make sure you subscribe to Fisher Phillips' Insight System to gather the most up-to-date information on the workplace.

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301
Email



Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

James Patrick
Partner
440.838.8800
Email

David J. Walton. CIPP/US

Partner
610.230.6105
Email

Service Focus

AI, Data, and Analytics

FCRA and Background Screening

Privacy and Cyber

Trending

AI Governance Hub