Job Applicants Sue AI Screening Company for FCRA Violations: 5 Key Takeaways for Employers

Insights
1.26.26

A new class action lawsuit against an AI recruiting platform could have significant implications for employers using artificial intelligence to screen job candidates. Two job applicants filed suit against Eightfold AI in California state court on January 20, alleging that the company violated federal and state consumer protection laws by creating "hidden credit reports" on job seekers without complying with statutory requirements imposed on consumer reporting agencies, including obtaining proper certifications from employment-purposed end-users. While we've started to see a series of lawsuits across the country attacking AI hiring systems for alleged discrimination, this could be the first to take the position that an AI tool could lead to a FCRA violation. Here's what employers need to know about this developing legal challenge and five key takeaways to help protect your organization.

The Allegations: AI Screening Tools as "Consumer Reports"

The lawsuit, filed by Erin Kistler and Sruti Bhaumik in Contra Costa County Superior Court, takes aim at Eightfold's AI-powered talent evaluation platform. The plaintiffs allege that when they applied for jobs at companies that use Eightfold's system, the platform assembled detailed dossiers about them using data far beyond what they provided in their applications.

According to the complaint, Eightfold's technology allegedly:

- Gathered information from third-party sources including LinkedIn, GitHub, Stack Overflow, and other public databases
- Analyzed data from "more than 1.5 billion global data points" including profiles of over 1 billion workers
- Created inferences about applicants' "preferences, characteristics, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes"
- Ranked candidates on a 0-5 scale based on their predicted "likelihood of success" in the role
- Provided these assessments to employers who used them to filter candidates before any human review

The core legal theory is that these assessments constitute "consumer reports" under the federal Fair Credit Reporting Act (FCRA) and California's Investigative Consumer Reporting Agencies Act (ICRAA), and that Eightfold failed to comply with the longstanding requirements these laws impose on companies that provide such reports. Eightfold responded to the allegations in a media statement saying that they "do not scrape social media and the like," so we'll see more information as the case unfolds.

The Legal Framework: 1970s Laws Meet 2020s Technology

The FCRA has regulated consumer reporting agencies since 1970, well before the advent of AI screening tools. But according to the lawsuit, Congress designed the law to evolve with technology and protect workers from opaque decision-making based on information they can't review or correct.

The statute defines "consumer report" broadly to include any communication "by a consumer reporting agency" about a person's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" that is used to evaluate their eligibility for employment. It covers far more than traditional credit checks – it was also designed to regulate third-party companies that assemble other types of information about people for use in high-stakes decisions like hiring.

When consumer reports are used for employment purposes, the FCRA requires:

- **Clear, written disclosure**: Job applicants or employees must receive a clear and conspicuous written disclosure, in a document that consists solely of the disclosure (i.e., stand-alone), that notifies the individual that a consumer report will be obtained for employment purposes
- **Written authorization**: Applicants (as well as employees) must authorize in writing the procurement of their consumer report
- **Pre-adverse action notice**: Before rejecting a candidate (or before taking adverse action against an existing employee) based on a consumer report, employers must provide the individual with a copy of the report and a copy of A Summary of Your Rights under the Fair Credit Reporting Act (*i.e.*, the CFPB's written description of the consumer's rights under the FCRA)
- **Adverse action notice**: After providing the pre-adverse action notice, if, after waiting a reasonable period of time, an employer decides to take an adverse action based on information in a consumer report, it must give the applicant or employee a notice of that fact and provide other statutorily required information.
- **CRA certifications**: Consumer reporting agencies must obtain certifications from employers that they, among other things, will comply (or, in some respects, have complied) with these requirements

California's ICRAA imposes similar and in some cases more stringent or additional requirements (as do other state and local laws).

The plaintiffs allege they received none of these protections when applying through Eightfold's platform. They claim they were never told that a consumer report would be created, never authorized its creation, and never had an opportunity to review or dispute the information before being rejected.

What Makes This Case Different

This isn't the first lawsuit challenging AI hiring tools; we've tracked discrimination claims against platforms like HireVue and Workday, just to name a few. But this case takes a different legal angle by focusing on consumer protection laws rather than bias claims.

The plaintiffs aren't arguing (at least in this lawsuit) that Eightfold's AI is discriminatory. Instead, they're arguing that the fundamental process of using AI to assemble third-party data about job seekers and rank them for employers triggers FCRA obligations that the company allegedly ignored.

This theory could have broad implications because it doesn't depend on proving the AI produces biased outcomes. If the courts agree that AI screening tools like Eightfold's create "consumer reports," then the companies providing these tools (and the employers using them) would need to comply with FCRA procedures irrespective of whether these tools are susceptible to bias or fairness challenges.

 NOTE: We identified this potential theory of liability in a 2024 Insight: "**Employers and Vendors Have FCRA Obligations When Using Workplace AI Tools: Your Step-by-Step Compliance Guide.**" We recommend you read this as a supplement to the Insight you're reading now, especially if you are an AI vendor.

The Employer Implications: 5 Key Takeaways

While this lawsuit targets the AI vendor rather than the employers who used its services, the case should prompt every employer using AI screening tools to evaluate their compliance posture. Here are five critical considerations:

1. Understand What Your AI Vendor is Actually Doing

Many employers may not fully understand the extent to which their AI recruiting platforms are pulling in external data to evaluate candidates. The Eightfold complaint describes a system that goes far beyond simply parsing the resume a candidate submits. The plaintiffs claim that it

allegedly searches the internet for additional information, compares candidates against billions of data points, and makes predictions about their future performance.

Ask your vendors detailed questions: What data sources are they using? Are they pulling information from outside the candidate's application? Are they making predictions or inferences about candidates based on comparisons to other workers? Are they providing you with scores or rankings? The answers will help you assess whether FCRA (as well as similar state and/or local) obligations may be triggered. You can find a list of questions to pose to your AI vendors here.

2. Review Your Vendor Contracts and Compliance Documentation

If your AI screening vendor is functioning as a consumer reporting agency, they should be obtaining the required certifications from you as the employer. These certifications confirm that you:

- Will and have provided standalone FCRA disclosures to the candidate
- Will and have obtained written authorization before procuring the report
- Will follow pre-adverse action procedures before rejecting a candidate
- Will not use the information in violation of equal employment opportunity laws or regulations

Review your vendor agreements (as well as other documents or processes tied to your use of these vendors) to confirm these certifications are in place. If they're not, or if you're unsure whether your current practices comply with FCRA requirements, it's time to audit your screening processes.

And remember: an AI vendor's interpretation or risk assessment relating to the potential application of the FCRA may not align with yours. Simply because the vendor says it does not believe the FCRA does not apply does not mean that that is true. You should conduct your own risk assessment as to whether the FCRA applies.

3. Don't Assume Your Current Background Check Process Covers AI Tools

Many employers have robust FCRA compliance programs for traditional background checks: criminal records, credit reports, employment verification, and the like. But AI screening tools may be operating in a different silo, perhaps managed by your talent acquisition team rather than your HR compliance function.

Make sure your FCRA compliance extends to all third-party screening tools, not just traditional background check vendors. This may require cross-functional conversations between HR, legal, compliance, and IT teams to map out all the platforms you're using and assess their compliance requirements.

4. Prepare for Increased Scrutiny of AI Hiring Tools

This lawsuit is part of a broader trend of legal and regulatory challenges to AI in employment. Federal and state agencies are paying close attention, and plaintiffs' attorneys are actively looking for test cases.

Even if you're confident your current practices are lawful, be prepared to explain and defend them. Document your compliance efforts, maintain records of vendor due diligence, and consider engaging counsel to review your AI hiring practices before a lawsuit or investigation arises.

5. Consider the Risks Even if You Think FCRA Doesn't Apply

Some employers and vendors may take the position that their AI screening tools don't create "consumer reports" subject to FCRA. They might argue that the tools only analyze information the candidate provided, or that the analysis is too integrated into the employer's own decision-making to constitute a third-party report.

These may be reasonable legal positions depending on the specific facts. But even if you're confident FCRA doesn't apply, consider the reputational and practical risks of using opaque AI tools to make hiring decisions. Candidates are increasingly concerned about algorithmic decision-making, and using tools that feel like "black boxes" could hurt your employer brand and ability to attract talent, even if they're technically lawful.

What Happens Next

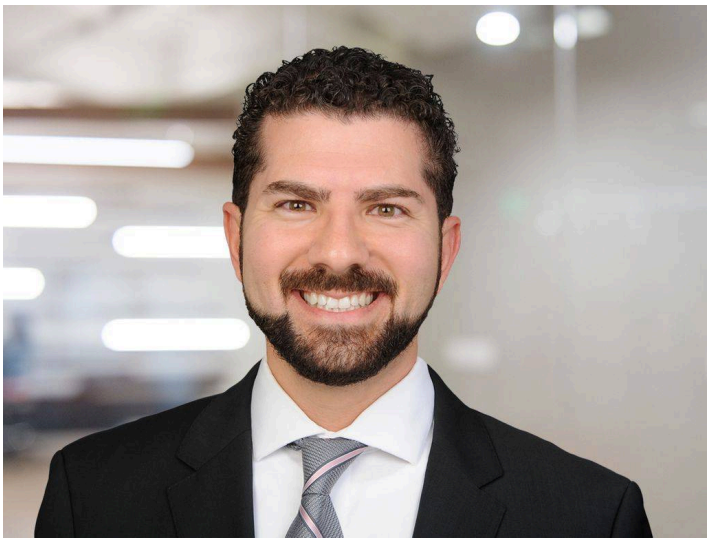
The Eightfold case is still in its early stages, and the company will have an opportunity to respond to the allegations. The legal issues are novel enough that the case could take years to resolve, potentially reaching appellate courts before there's a definitive answer on whether AI screening tools like Eightfold's constitute consumer reports subject to FCRA.

In the meantime, other AI vendors and the employers who use their tools will be watching closely. If the plaintiffs succeed in establishing that these platforms trigger FCRA obligations, it could reshape how AI is used in hiring across the country.

Conclusion

We will continue to monitor developments in this case and other legal challenges to AI hiring tools. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions about your organization's use of AI in recruiting or hiring, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our AI, Data, and Analytics Practice Group, our Privacy and Cyber Practice Group, or our FCRA and Background Screening Practice Group.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

James Patrick
Partner
440.838.8800
Email

Service Focus

AI, Data, and Analytics

FCRA and Background Screening

Privacy and Cyber

Litigation and Trials