Employers Beware: Uptick in BIPA Lawsuits Targeting AI Note-Taking Software

Labor & Employment Law Update

By Ryan Young on February 11, 2026

A new wave of litigation under the Illinois Biometric Information Privacy Act (BIPA) has emerged, zeroing in on a technology many employers now routinely use: AI-powered meeting transcription and note-taking tools.

In recent months, plaintiffs have filed class actions alleging that vendors like Fireflies.AI collect and store "voiceprints"—unique biometric identifiers derived from speech—without providing the written notice, informed consent, or transparent retention and destruction policies BIPA demands. One such case is *Cruz v. Fireflies.AI Corp.* in the Northern District of Illinois. The complaint asserts that the software recorded, analyzed, and retained participants' voices, including those of non-users, without satisfying BIPA's statutory prerequisites.

Why AI Transcription Tools Are Drawing Scrutiny

This uptick in lawsuits isn't isolated. Under BIPA's broad definition of biometric data, voiceprints—like facial scans or fingerprints—may qualify as biometric identifiers. Many AI meeting assistants automatically join virtual meetings, distinguish between speakers, and generate attributed transcripts. As a result, they are increasingly in plaintiffs' crosshairs because collecting such identifiers triggers strict procedural requirements *before* data collection. Additionally, many AI notetaking tools in widespread use lack clear mechanisms for disclosing biometric collection to all participants or securing their written consent, leaving vendors and their customers exposed.

Employer Liability: More Than Just the Vendor at Risk

Although the initial litigation often names the AI technology provider as a defendant, employers that deploy these tools aren't insulated from liability. Illinois courts have held that multiple entities can be responsible for the same biometric collection when they enable, authorize, or benefit from the technology's use. An employer that licenses or encourages the use of an AI notetaker in business meetings—or whose employees activate such software during meetings involving Illinois residents—may be implicated in BIPA claims if proper safeguards aren't in place. This risk extends even to organizations headquartered outside Illinois if any meeting participant is physically located in

the state.

Three Tips to Protect Employers From BIPA Exposure

To reduce legal risk, employers should:

1. **Implement clear policies** governing the use of AI meeting tools. This entails cataloging which transcription or notetaking apps are permitted, determining whether they collect biometric data, and restricting who can enable them in meetings that include external parties or individuals located in Illinois.
2. **Build a robust consent framework** by notifying all participants that biometric data may be collected, specifying how long it will be retained, and obtaining their informed, written consent before any such data capture occurs.
3. **Partner with vendors** to ensure they have compliant notice, consent, and data retention/destruction practices, but don't outsource responsibility. Employers should conduct their own due diligence and document compliance efforts in case of litigation.

By proactively governing AI notetaking technologies, employers can harness productivity gains without overlooking the considerable privacy risks that have made BIPA one of the most litigated biometric privacy statutes in the nation.