

THE RISING TIDE OF BIPA CLAIMS



WORLD WIDE
Specialty Programs

World Wide Specialty Programs, Inc. • World Wide New York Insurance Services, Inc. • CA, NH, TX

THE RISING TIDE OF BIPA CLAIMS

What it is, how it impacts your business, and where coverage is – or isn't. Is your staffing firm protected?

Thanks to a recent Illinois Supreme Court ruling, businesses everywhere – particularly staffing firms – have been put on notice.

The state's stringent 2008 Biometric Identifier Privacy Act (BIPA) means that personally identifiable information is the same no matter what form it takes on. That's the message derived from a recent ruling in Illinois Supreme Court on a case involving BIPA regulation. In the case involving a 14-year-old plaintiff, the Court held that Six Flags violated BIPA by requiring a fingerprint in order to obtain a season pass.

The decision held that an individual alleging that a violation in the state's laws regarding biometric information – defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" – is already "real and significant" when it occurs. Plaintiffs do not need to prove actual harm, says the Court, but only that a violation has occurred.

The Court's action has put staffing firms in the crosshairs, particularly since they are responsible for their employees' personal data no matter where they are working. It's an impact that is compounded by not just the policies and practices of the staffing firm, but also very much by the policies and practices of client firms.

If you don't think it's impacting business, think again. The Illinois decision may well influence other legal action brought by employees against their companies. In one ongoing class action suit, a hotel worker was required to scan his fingerprint into biometric time-tracking devices to clock in and clock out of his shifts. The worker alleges that his employer did not seek his permission to collect, use, store, or disseminate his biometric information, nor was there a written policy on biometric information retention or sharing.

In another case, employees of a major airline are alleging the same type of time-keeping scanning was occurring without permission or any written policy. This, also a class action suit, includes employees whose biometrics were captured, collected, obtained, stored, or used by the airline in the state of Illinois. The suit was later tossed by a federal judge on other grounds.

It's not just a local issue, either. Despite BIPA being an Illinois regulation, its impact is being felt far afield. Any company doing business in Illinois, no matter where it is domiciled, must comply with the regulation.

And while BIPA has not been widely adopted, two other states – Washington and Texas – have enacted similar biometric privacy legislation. As of this writing, Massachusetts, New York, Delaware, Alaska, Michigan, and other states are considering their own biometric privacy legislation.

HOW IT IMPACTS STAFFING FIRMS

For staffing firms, that means the time to address biometric privacy is now. Staffing firm employees going to a client that is using biometrics is the responsibility of the staffing firm. Any violations resulting in claim or legal action would be charged against the staffing firm's employment practices liability (EPL) insurance, not that of the client employer's.

That means it's not enough for staffing firms to rely solely on their own biometric information policies and permissions. Staffing firms must now understand the policies and practices of all employer companies that their employees work with. Without that due diligence, a staffing firm could find itself on the receiving end of a costly EPL claim.



WAYS TO PROTECT YOUR STAFFING FIRM

Staffing firms need to be addressing the risk now. Here are ways to reduce your risks and protect your business and employees:

- ✓ Ask each client company to provide information on their use of biometric scanners as well as a copy of its biometric policy.
- ✓ Inform all staffing employees that if they are asked for any biometric data by a client, the employee must call staffing firm before they agree to provide such biometric data. Your staffing firm should have a dedicated number and designated employee to call for employees to call regarding these client requests.
- ✓ Require clients to keep you informed of any addition of or amendment to their use of biometrics.
- ✓ Establish a policy to inform all potential employees or temp workers either working with or interviewing with client companies of their use of biometric identification prior to the worker visiting the client.
- ✓ Use state-specific written releases to inform and gain consent from workers prior to their visiting the client that they understand and agree to the client's use of biometric identification tools.
- ✓ Inform workers of the specific purpose and length of term for which the employee's or interviewee's biometric identifiers and/or biometric information will be collected, stored, and/or used.



COVERED OR NOT?

Also, staffing firms should be reviewing their employment practices coverage with their insurer to understand what is covered and what is not. In most cases, standard EPL policies do not necessarily include coverage for biometric information violations. And cyber policies will most likely not protect for this cause of action, and will not cover for your clients' use of biometrics.

Be aware that not all brokers know about or understand the rules regarding biometric privacy and data use. Talk with an insurer or broker who specializes in your industry, and who has demonstrated an understanding of the issue.

If your state doesn't have biometric privacy laws today, that can and will most likely change. Regardless, all staffing firms should be addressing the risks now in order to stay compliant. What you do today could protect you from future claims, and can go a long way toward keeping your workers' personal information safe.



**For more information on The Rising Tide of BIPA Claims,
contact World Wide Specialty Programs at
1-877-256-0468.**