Client Advisory

Employment Related Risks

Biometric Information Privacy Act (BIPA)

What It Is and Why It Is Important

The Illinois Biometric Privacy Act ("BIPA") was enacted in 2008 to regulate how private companies collect, use, safeguard, retain, destroy and share defined biometric data of employees and third parties.[1] An individual biometric identifier, such as a fingerprint or retina scan, is unique to each person and the legislature wanted to protect this data.

Frequency of risk. Although the law has been on the books for some time, it has gained traction in recent years as private companies utilize technology more frequently to track employees and/or consumers. More than 250 BIPA lawsuits were filed in 2022 alone and that trend shows no sign of slowing down. Both employers/end-users and vendors/technology providers have been sued under BIPA.

According to a study from the Chamber of Progress, 88% of all BIPA lawsuits are employer-employee disputes stemming from the use of biometric timekeeping systems.

Severity of risk. The BIPA statute provides for liquidated damages of $1,000 per negligent violation and $5,000 per reckless violation. Consider the number of times customers or employees may have encountered a violation, sometimes on a daily basis, over a long period of time. As a result, the Act has attracted the interest of the plaintiff's bar for class action lawsuits. The litigation surrounding BIPA continues to evolve and it is critical for companies to stay current on the exposure, legal trends, and implications.

Focus on Employment Risk

Biometric identifiers under BIPA include retina/iris scans, fingerprints, voiceprints, hand or face scan, or face geometry. Biometric information is any data — regardless of how it is captured, converted, stored, or shared — based on an individual's biometric identifier used to identify an individual. Employers sometimes use biometric identifiers to track employees clocking in and out of work, providing security

access to buildings and equipment. Biometric identifiers have also been utilized in connection with COVID-19 or other health screenings.

What Is at Risk – Statutory or Actual Damages

Individuals can file a lawsuit which provides for recovery of damages. For negligent violations, the statute provides for liquidated damages of $1,000 or actual damages, whichever is greater. For intentional or reckless violations, the statute provides for liquidated damages of $5,000 or actual damages whichever is greater.

If a company has 500 employees working 200 days a year, they are typically undergoing 4 retina scans per day per employee (arriving to work, returning from morning break, returning from lunch, returning from afternoon break). At $1,000 per negligent violation, that amounts to $400,000,000 — a staggering number.

Continued on next page

Recent Case Law Expands Potential Exposure

The landmark Illinois Supreme Court case of *Rosenbach v. Six Flags Entertainment Corp.* found that no actual injury or adverse effect, beyond the violation of an individual's rights under BIPA, must occur for a plaintiff to have standing to sue.

In February 2023, the Illinois Supreme Court held in *Cothron v. White Castle* that a separate claim accrues under BIPA ***each*** time a private entity scans or transmits a person's biometric identifier or information in violation of the law. This is alarming because multiple violations can be linked to a single individual, potentially raising exposure to catastrophic levels. Earlier the same month, on February 2, 2023, the Illinois Supreme Court ruled in *Tims v. Black Horse Carriers, Inc.* that a ***five-year*** limitation period applies to all claims arising under BIPA. This could significantly increase potential damage calculations for violations of BIPA.

Other Applicable Laws

In addition to BIPA, the CCPA (California Consumer Privacy Act), GDPR (The European Union's General Data Protection Regulation), and some state privacy regulations contain provisions surrounding the unlawful collection of personal information that is shared with third-party vendors without proper disclosure and releases.[2]

Best Practices for Employers

Prevention is always the best medicine. Employers should:

- Have a written policy, available to the public, which establishes a retention schedule and guidelines for permanently destroying biometric identifiers and information.
- Inform individuals in writing that a biometric identifier is being collected or stored, and the purpose and length of time for which biometric information is being collected, stored, and used.
- Receive a written release from the individual.
- Refrain from selling, trading, leasing or otherwise profiting from a person's biometric information.
- Refrain from disclosing, redisclosing, or otherwise disseminating a person's biometric information unless consent is provided.
- Use reasonable standards of care in storing, transmitting, and protecting from disclosure biometric identifiers consistent with the standard of care within the company's industry, and in a manner that is more protective than the manner in which the company stores, transmits, and protects other confidential and sensitive information.

Insurance Implications

Multiple coverages may come into play for this exposure, notably employment practices liability (EPL), cyber insurance, and, perhaps, directors & officers (D&O) liability.

As courts have allowed class members to sue for violations of BIPA without the existence of harm, and with litigation and nuclear (historic highs) verdicts on the rise, EPL insurance carriers began to take note and carve back or exclude coverage for biometric information claims and limit their own risk exposure to companies collecting employee biometric data. Some EPL carriers cap losses via sub-limit, provide only defense costs, or address losses in the underwriting process in the form of a specific BIPA-targeted questionnaire.

Further, depending on the type or the timing of allegations, certain exclusionary language in typical EPL policies may come into play. For example:

- A bodily injury exclusion may preclude or limit the breadth of coverage, or
- Pending or prior litigation, prior notice, or prior acts exclusions may limit or preclude coverage.

Employers should discuss insurance implications with their USI Insurance Services account service team and review any current and future EPL policies.

Director and Officer (D&O) Insurance

Directors and officers (D&O) liability policies cover exposures faced by directors, officers, and the company itself that arise from alleged wrongful acts in the management of the company. D&O coverage could potentially be implicated if there are allegations of failed oversight, like not following BIPA requirements and safeguarding employee or third-party data. However, common exclusions in these policies for invasion of privacy, employment practices, or insured versus insured claims could preclude any coverage.

Continued on next page

Look to Cyber Insurance

Some cyber insurance policies may include coverage for privacy violations or data breaches that involve biometric information.

Cyber insurers are increasingly concerned with the wrongful collection of personal information. The primary source of this concern is the enforcement action taken by the Federal Trade Commission (FTC) against several healthcare companies like GoodRX, BetterHealth, and Mass General which are not regulated by the Health Insurance Portability and Accountability Act (HIPAA) and Office for Civil Rights/ Health and Human Services (OCR)/HHS).

As a result, cyber insurance carriers are asking supplemental questions on the use of tracking technologies, privacy notices, and employee training during the underwriting and renewal process.

Several insurance carriers have drafted exclusionary language intended to be used on policies for non-compliant companies.

It is important to carefully review the policy language and consult with an experienced insurance broker or legal counsel to determine whether BIPA claims are covered under a particular cyber insurance policy. Even if a policy provides coverage for BIPA claims, certain exclusions or limitations may apply.

Employers need to be aware of the use of these technologies within their organizations. They should confirm the appropriateness of privacy policies and compliance with those policies within the organization to any applicable regulations.

How USI Can Help?

We work closely with our clients as they navigate the evolving employment law environment. We further recommend that employers consult with counsel to assess and monitor federal, state, and local employment laws.

We also prepare clients to respond to targeted questions from EPL or Cyber underwriters, and negotiate with insurers to obtain the broadest EPL, Cyber and other policy language.

For more information, please contact your local USI consultant, or visit us at www.usi.com.

Sources:

[1]Texas and Washington have enacted their own similar data privacy laws (although there is no private right of action and only the state attorney general may bring an action. Other jurisdictions have addressed in their general privacy protection statutes. While the statutory requirements and restrictions differ in laws regulating biometric data, common themes include:

- Requiring some form of notice: – that the entity collects biometric information; and – about how the entity uses the information.
- Requiring clear consent from the individuals to use their biometric data, sometimes in writing.
- Restricting to various degrees the sale, lease, or other disclosure of biometric information.
- Providing standards for confidentiality, retention, and data disposal when an organization no longer needs biometric information for the collection purpose.

[2]On May 22, 2023, it was announced that Meta has been fined a record-breaking €1.2 billion ($1.3 billion) by European Union regulators for violating EU privacy laws by transferring the personal data of Facebook users to servers in the United States.