Crowell

Client Alert

BIPA Claims Uniformly Have a 5-Year Statute of Limitations

February 6, 2023

Key Takeaways

1. A Potential Increase in Claims, Costs and Damages
2. Reduce Liability Through Transparency

On February 2, 2023, the Illinois Supreme Court ruled that all Biometric Information Privacy Act ("BIPA") claims are uniformly subject to a five-year statute of limitations, expanding liability for businesses collecting biometric information.[1] In *Tims v. Black Horse Carriers, Inc.,*the court found that a longer, uniform statute of limitations for all claims under BIPA best fulfilled the legislative intent to hold private entities accountable and provide redress for data subjects.[2] The *Tims* decision partially reversed an appellate court's interlocutory decision that applied a one-year statute of limitations to some sections of BIPA, while applying a five-year statute of limitations to others.[3] This highly anticipated decision will allow companies to understand and manage their liability risk and will also likely fuel the growth of future BIPA lawsuits.

Background

The matter arises from a class action lawsuit filed by Jorome Tims against his former employer, Black Horse Carriers, Inc. ("Black Horse"), alleging that when Black Horse scanned his fingerprints, the company violated BIPA sections 15(a), 15(b), and 15(d).

The Illinois Biometric Information Privacy Act is the country's first comprehensive biometric privacy legislation. BIPA contains five obligations for private entities collecting biometric information:

- 15(a) requires entities to develop and make public an information retention policy;
- 15(b) prohibits a private entity from collecting biometric information without first obtaining informed consent from the data subject;
- 15(c) prohibits a private entity from profiting from the sale of biometric information;
- 15(d) prohibits disclosure of biometric information without the consent of the subject; and
- 15(e) requires entities to protect biometric information from disclosure.[4]

Statutory damages can be steep and add up quickly, accruing per violation.[5] A company that negligently violates a provision of BIPA is liable for damages of $1,000 per violation, while a company that intentionally or recklessly violates a provision is liable for damages of $5,000 per violation.[6] Plaintiffs are also entitled to pursue attorney fees, and actual damages in the event the actual damages are higher than the statutory amount.[7] The courts are currently evaluating what is considered a violation under BIPA, in particular, whether

BIPA liability accrues per data subject or per incidence – in other words, per scanned employee or per fingerprint. At up to $5000 per violation, a per incident accrual would significantly increase possible damages for entities collecting biometric data and make even small businesses liable for huge sums.

Illinois Supreme Court Decision

The Illinois Supreme Court relied on legislative intent to determine the statute of limitations for BIPA claims in *Tims*.[8] The court declined to apply two different limitations as to "reduce uncertainty and create finality and predictability."[9] The court contemplated the practical impact of multiple time constraints, noting that "[t]wo limitations periods could confuse future litigants about when claims are time-barred, particularly when the same facts could support causes of action under more than one subsection of [BIPA]." Considering "the intent of the legislature, the purposes to be achieved by the statute, and the fact that there is no limitations period in [BIPA]," the court found that the five-year catchall limitation period would best apply.[10] The court believed policy considerations were best served by a longer limitation period because of "the fears of and risks to the public surrounding the disclosure of … biometric information." The longer limitation period would enhance the ability for an aggrieved party to seek redress and lengthen the time a company could be held liable of noncompliance.[11]

Key Takeaways

***A Potential Increase** in Claims, Costs and Damages*

The expansion of liability resulting from the extended five-year statute of limitations will open the door to an increased number of BIPA actions, expanding both the number of possible plaintiffs and the number of possible claims. All BIPA cases that had been stayed awaiting the *Tims* decision will now be allowed to proceed under the expanded statute of limitations. Additional cases may be brought that had previously been outside the one-year limitation. Further, cases that would have once excluded claims under 15(c) and 15(d) due to the one-year limitation may now be expanded to include such claims. Litigation under the expanded statute of limitations may be costlier given the likely increase in claims. Additionally, because damages accrue per violation under each claim, defendants may see damages increase significantly.

Reduce Liability Through Transparency

Organizations contemplating the use of biometric technologies for personnel management should be thoughtful about transparency in their implementation, for example by (i) providing employees with the opportunity to consent to biometric data capture, and (ii) publishing a robust privacy policy that outlines the use and retention of their biometric information. A majority of the biometric litigation filed over the past two years have largely been based on the issue of notice and organizations can significantly mitigate their risk by establishing a culture of transparency in their business.

* * *

Crowell & Moring LLP has a robust and highly experienced team advising organizations of all sizes on compliance with biometric privacy laws. Crowell also has an extensive library of resources associated with the Illinois Biometric Privacy Act, including:

A Statute of Limitations for BIPA Claims? We May be One Step Closer

Ninth Circuit Rejects Facebook's Article III Argument; Biometric Lawsuit Will Proceed

Illinois' First Settlement under Biometric Law; AMA Adopts Principles for Mobile Health Apps; Ecuador to Enact Data Privacy Law

---

[1] *Tims et al. v. Black Horse Carriers Inc.*, case number 127801, at 10.

[2] *Id.*

[3] *Tims v. Black Horse Carriers, Inc.*, 184 N.E.3d 466 (2021).

[4] 740 ILCS 14/15.

[5] 740 ILCS 14/20.

[6] *Id.*

[7] *Id.*

[8] *Tims et al. v. Black Horse Carriers Inc.*, case number 127801.

[9] *Id* at 5.

[10] *Id* at 11.

[11] *Id* at 13.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com

Jason Stiehl
Partner – Chicago

Phone: +1.312.840.3108
Email: jstiehl@crowell.com

Laura Foggan
Partner – Washington, D.C.
Phone: +1.202.624.2774
Email: lfoggan@crowell.com

Christiana State, CIPP/US, CIPP/E
Senior Counsel – San Francisco
Phone: +1.415.365.7431
Email: cstate@crowell.com

Garylene (Gage) Javier, CIPP/US
Associate – Washington, D.C.
Phone: +1.202.654.6743
Email: gjavier@crowell.com

Alexis Ward
Associate – Los Angeles
Phone: +1.213.271.2797
Email: award@crowell.com