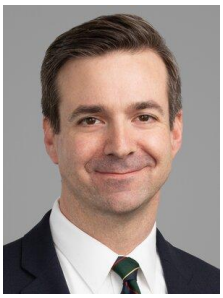
Financial Industry Must Beware Rising BIPA Litigation Tide

By **Charles DeVore, Geoffrey Young and Anna Mikulski** (June 1, 2023)



Charles DeVore

Geoffrey Young

Anna Mikulski

In recent years, litigation under the Illinois Biometric Information Privacy Act has become one of the top class action trends in the U.S. — and this trend has accelerated on the heels of two pivotal decisions by the Illinois Supreme Court in the first quarter of 2023.[1]

While BIPA litigation has focused primarily on employers using fingerprint biometrics for timekeeping purposes, class action plaintiffs firms — spurred on by a significant expansion of available damages for biometric privacy suits recently — have sought new targets for BIPA litigation, including the financial industry.

As discussed in this article, BIPA's exemption for financial firms and their affiliates has been challenged in multiple cases, with some courts beginning to limit its application.

BIPA Overview

BIPA is the most expansive biometric privacy law in the country, and has strict requirements for businesses collecting, storing or using biometric data — including voiceprints, fingerprints and facial scans.[2]

While other states have passed comprehensive consumer privacy laws that implicate biometric information, currently only three states — Illinois, Washington and Texas — have enacted their own biometric-specific privacy laws.

Only Illinois' BIPA provides individuals with a private right of action that can result in substantial liability for companies collecting and handling biometric information, ranging from $1,000 for each negligent violation to $5,000 for each intentional or reckless violation.

Enacted in 2008, BIPA has significantly evolved over the past few years with class action plaintiffs attorneys pursuing hundreds of class actions in both state and federal courts.

In the last two months alone, the number of lawsuits in Illinois circuit courts alleging BIPA violations — which was already on the rise — has increased by approximately 65%.[3]

This recent explosion of BIPA litigation has been prompted by two long-awaited Illinois Supreme Court decisions that exponentially expanded the available damages for BIPA violations.

First, on Feb. 2, the Illinois Supreme Court issued its opinion in Tims v. Black Horse Carriers Inc.,[4] where the court rejected the intermediate appellate court's ruling that a one-year limitations period applies to claims brought under those sections of BIPA that involved publication of biometric data — i.e., Sections 15(c) and 15(d) of BIPA.

Instead, the court held that a five-year limitations period applies to all BIPA claims, including those involving publication of biometric data.

Shortly thereafter, on Feb. 17, the Illinois Supreme Court held in Cothron v. White Castle System Inc. that every instance of collecting or using biometric data — rather than just the first instance for a given plaintiff — constitutes a compensable injury under BIPA.[5]

According to the court, the plain language of BIPA's requirement that prior informed consent is necessary before capturing, using, disclosing or disseminating biometric information applies separately to each and every capture or use of this data.

Because BIPA claims are often based on repeated actions — such as fingerprint scanning to clock in and out during the workday or repeated identity verifications for transactions, defendants face potentially astronomical damages following Cothron.

The court recognized, but was not dissuaded by, the potential for outsized damages, finding that the statutory language was clear and explaining that it "continue[s] to believe that policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature."[6]

Limits of the GLBA Exemption Under BIPA

In the wake of the Tims and Cothron cases, there has been a notable uptick in BIPA class action filings, and the filings reflect that plaintiffs attorneys are expanding the nature of the cases they are pursuing given the potential for lottery-ticket-sized awards.

Until recently, financial institutions have largely been able to avoid the explosion of BIPA litigation due to an express statutory exemption under BIPA, which states that the statute does not

> apply in any manner to a financial institution nor an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.[7]

The GLBA exemption's affiliate language expands the scope beyond traditional financial institutions to essentially any entity subject to the GLBA's privacy related requirements — commonly known as the financial privacy rule.[8]

Courts have consistently held that the definition of financial institution under BIPA is the definition set forth in the GLBA, which is broad and encompasses "any institution the business of which is engaging in financial activities."[9]

These financial activities include lending, exchanging, transferring, investing for others; safeguarding money or securities; providing financial, investment or economic advisory services; and underwriting, dealing in or making a market in securities.[10]

For example, in November 2022, the U.S. District Court for the Northern District of Illinois dismissed BIPA claims brought against DePaul University, holding that the university was a financial institution because it engages in student aid and lending funds.

It noted that at least five other courts have also concluded that "institutions of higher education that are significantly engaged in financial activities such as making or

administering student loans" qualify for the exemption.[11]

Although the GLBA exemption has traditionally been viewed as a robust defense to BIPA claims, the exemption is not boundless and recent decisions indicate that courts may limit its applicability.

In stark contrast to the DePaul University case noted above, in Patterson v. Respondus Inc., the Northern District of Illinois denied Lewis University's motion to dismiss premised upon the GLBA exemption.[12]

There, the court was unconvinced that Lewis University was subject to the GLBA because the university relied on general statements made by the Federal Trade Commission that universities are financial institutions rather than presenting any evidence that the university itself is "significantly engaged in lending funds to consumers."

Thus, merely claiming to be a GLBA-regulated entity is not enough to procure dismissal.

Recent court decisions also demonstrate that financial industry players may be at risk for BIPA exposure based on the conduct and practices of their vendors. Plaintiffs attorneys have recently found traction targeting the practices of vendors that financial institutions utilize for identity verification, including via fingerprints, facial scans and voiceprints.

Third-party vendors that process biometric data on behalf of financial institutions may still face liability in spite of the GLBA exemption.

In Davis v. Jumio Corp.,[13] the court rejected defendant Jumio's motion to dismiss based upon the GLBA exemption. Jumio was a vendor providing identity verification for users of the cryptocurrency exchange Binance Holdings Ltd. through an application.

Rather than contending that it was a financial institution protected by the GLBA exemption, Jumio argued that Binance was a qualifying financial institution, and entertaining BIPA liability related to verifying the identity of the crypto exchanges' customers would effectively impose BIPA requirements on the exchange in contravention of the GLBA exemption.

The court ruled that there was insufficient evidence demonstrating that Binance was a qualifying financial institution under the GLBA exemption. Critically, the court also questioned whether the GLBA exemption could apply to Jumio simply because it was a vendor of a qualifying financial institution.

Notably, in McGoveran v. Amazon Web Services Inc. in the U.S. District Court for the District of Delaware in March, an identity-verification vendor successfully argued that it satisfied GLBA's definition of financial institution, and thus was exempt from BIPA claims.[14]

As BIPA litigation engulfs more financial institutions, it is important that these institutions evaluate and understand their practices — and their vendors' practices — for collecting, handling and storing biometric information. Likewise, it is important for financial institutions to consider whether their vendors can or should comply with BIPA's requirements.

Financial institutions also would be wise to revisit their indemnity agreements with vendors involved in collecting and handling biometric information, as litigation is a distinct possibility.

Although the GLBA exemption provides a possible defense from BIPA claims, financial institutions and their vendors should take steps to bolster compliance and be poised to prove the applicability of the GLBA exemption if they are targeted with a BIPA action.

Beyond BIPA: The Rise of Biometric Litigation Under California Law

While Illinois' BIPA is the dominant law in the biometric privacy legal landscape, some California laws also pose a significant risk of biometric data class actions brought against financial institutions.

For instance, the California Consumer Privacy Act, although not exclusively a biometric privacy statute, governs the processing of biometric data, and imposes requirements on entities collecting and using the biometric information of California residents.[15]

Notably, CCPA's financial industry exemption is much narrower than BIPA's, providing only a partial exemption for information collected by financial institutions where the specific data itself is subject to the GLBA.[16] Such information, although exempt from the privacy requirements of the CCPA, is not exempt from the private right of action for data breaches.

Despite this relatively limited private right of action, plaintiffs attorneys have filed numerous class actions using alleged CCPA violations as a predicate for causes of action under California's plaintiff-friendly Unfair Competition Law.

As with the overall increase of privacy litigation in the U.S., there has been an upward trend in the number of CCPA filings to date, including an increase in the number of cases brought against financial institutions.

Although many of these cases are in their initial stages, rulings on pending motions to dismiss will provide further guidance on the pleading requirements and limits of CCPA-related claims.

Another growing trend in biometric privacy litigation rooted in California law is class action litigation targeting voice authentication technology by alleging the practice violates California's Invasion of Privacy Act, a statute originally enacted for the purpose of preventing the recording of phone calls.[17]

The CIPA provision at the center of this new wave of class action litigation bars "any system which examines or records in any manner voiceprints or other voice stress patterns of another person to determine the truth or falsity of statements made by such person" without written consent "in advance of the examination or recording."[18]

Complaints filed under this provision typically allege that companies are recording customers and analyzing their voiceprints later on for identity authentication purposes without first obtaining consent. Initial court rulings related to this novel theory of liability are beginning to trickle in.

In February, in Balanzar v. Fidelity Brokerage Services LLC, the U.S. District Court for the Southern District of California dismissed a complaint filed against Fidelity Brokerage for failing to sufficiently allege that the broker-dealer's authentication system determined the truth or falsity of any statements.[19]

The court found that the authentication system as alleged in the complaint was more akin to a biometric passcode than a lie detector, which is the focus of CIPA.

As class action plaintiffs firms continue to leverage CIPA for conduct that goes beyond the original purpose of the statute, financial firms and other companies that have been using voice authentication technology for customer security and privacy purposes should consider CIPA's consent requirement moving forward.

Charles A. DeVore and Geoffrey G. Young are partners, and Anna Mikulski is an associate, at Katten Muchin Rosenman LLP.

[1] 740 ILCS 14/1, et seq.

[2] 740 ILCS 14/10, 14/15.

[3] Stephen Joyce and Skye Witley, Illinois Biometric Privacy Cases Jump 65% After Seminal Ruling (May 2, 2023), https://news.bloomberglaw.com/business-and-practice/illinois-biometric-privacy-cases-jump-65-after-seminal-ruling?.

[4] 2023 IL 127801.

[5] 2023 IL 128004.

[6] Id. at ¶ 43.

[7] 740 ILCS 14/25(c).

[8] 15 U.S.C. §§ 6801-09.

[9] 15 U.S.C. § 6809(3)(A)

[10] 12 U.S.C. § 1843(k)(4) (enumerating various types of activities "considered to be financial in nature").

[11] Powell v. DePaul University, No. 21 C 3001, 2022 WL 16715887 (N.D. Ill. Nov. 4, 2022).

[12] 593 F. Supp. 3d 783 (N.D. Ill. 2022), reconsideration denied, No. 20 C 7692, 2022 WL 7100547 (N.D. Ill. Oct. 11, 2022).

[13] No. 22-CV-00776, 2023 WL 2019048 (N.D. Ill. Feb. 14, 2023).

[14] See McGoveran v. Amazon Web Servs., Inc., No. 1:20-CV-01399-SB, 2023 WL 2683553 (D. Del. Mar. 29, 2023).

[15] Cal. Civ. Code §§ 1798.100-96.

[16] Cal. Civ. Code § 1798.145(e).

[17] Cal. Penal Code §§ 630–638.

[18] Cal. Penal Code § 637.3(a).

[19] Balanzar v. Fid. Brokerage Servs., LLC, No. 22-CV-1372-GPC, 2023 WL 1767011 (S.D. Cal. Feb. 3, 2023).