HB 259 - Biometric Identifiers Privacy
Testimony of ADP, Inc.
February 2, 2022

ADP is the nation's largest payroll and human resources service provider, paying roughly one out of every six workers in the United States. ADP provides a range of administrative solutions to more than 600,000 U.S. clients, which enable employers of all types and sizes to manage their employment responsibilities from recruitment to retirement, including employment tax administration, human resource management, benefits administration, time and attendance, retirement plans, and talent management.

We are very concerned about the bill as written, largely based on adverse and unintended impacts of similar legislation enacted in Illinois. Despite not being a concern and not being referenced at all in the legislature's findings in the Illinois Biometric Information Privacy Act, **roughly 90% of the 250+ class action lawsuits filed under the IL BIPA since 2017 were related to timeclocks**.

The Biometric Information Privacy Act (BIPA) should exclude biometric information used exclusively in the employment context for employment, human resources, compliance, payroll, identification, authentication, safety, security, or fraud prevention purposes.

A brief explanation follows, along with specific issues and recommendations for this bill below.

- Many employers use finger-scan and hand-scan timeclocks to accurately record employees' time worked. These systems do not collect, store, or use fingerprints or handprints, but rather convert the scans into an encrypted series of numbers linked to an employee badge number. They also do not store employee names, or personal or financial information. The data used and stored by the timeclocks is encrypted and secure, and in any event cannot be used to steal employees' identities or to access personal or financial information.

- In effect, the Illinois BIPA resulted in very substantial harm to countless businesses in the state without any offsetting benefit. Employees knew their fingertips are being scanned, and the purpose of that scanning. Yet the law permitted enabling aggressive plaintiffs' attorneys to seek out common time-keeping systems for failures to meet the statutory disclosure and consent requirements, and to seek huge statutory penalties with no requirement to demonstrate any harm. The proposed BIPA in Maryland follows the Illinois law closely and would result in the same catastrophic economic harm.

- The Illinois Supreme Court affirmed that plaintiffs need not demonstrate any injury to seek liquidated damages of $1,000 per violation, and $5,000 for intentional or reckless violations.

- Applying such liquidated damages to timeclocks in the employment context through class action litigation yields astronomical potential liabilities which would threaten Maryland employers. Any violation is multiplied by the number of employees, times two or more timeclock transactions per day, times the number of days in as much as five years. **An employer with 20 employees could face claims of $100 million. An employer with 1,000 employees could see lawsuits seeking $5 billion**. Such huge potential liabilities were used to pressure countless employers into costly settlements.

- These lawsuits could wipe out smaller employers. Even if larger companies potentially could absorb the losses, it may force them into deep cost-cutting, including layoffs. In addition, Maryland employers may avoid using current timekeeping technologies – and would not be able to take advantage of reduced costs, greater accuracy and efficiencies.

- The bill provides that compliance would be easily accomplished by making a disclosure and obtaining a written release as a condition of employment, from each employee. Any such consent requirement as a condition of employment would be difficult and would result in job losses. Further, employers that are parties to collective bargaining agreements cannot unilaterally require employees to provide a written release as a condition of employment.

- Timekeeping system vendors would not generally be able to directly make disclosures and obtain written consents. Vendors have no employment or contractual relationship with the employees using the timeclocks, no rights to communicate with the employees to provide disclosures, and no ability to require employees to execute a written release as a condition of employment.

Proposed Exclusion from the Biometric Information Privacy Act

Maryland HB 259 should be amended to expressly remove timeclocks from the scope of the statute, **provided** that: (1) any biometric identifiers or biometric information collected or captured are used only for workplace timekeeping and/or payroll purposes, and are not transmitted or otherwise provided to any person or entity for any other purpose; *and* (2) all entities in possession of biometric identifiers or biometric information store, transmit, and protect such biometric identifiers or biometric information in a manner that is the same as or more protective than the manner in which they store, transmit, and protect confidential and sensitive information.

Proposed Amendment:

Nothing in this Act shall apply to any biometric identifiers or biometric information collected, captured, used, stored, or transmitted in the context of employment, including human resources, compliance, payroll, identification authentication, safety, security, or fraud prevention purposes, *provided that* any private entity that collects, captures, uses, possesses, transfers, and/or receives any such biometric identifiers or biometric information:

(i) does so exclusively for such purposes;

(ii) does not sell, lease, or trade such biometric identifiers or biometric information; and

(iii) stores, transmits, and protects such biometric identifiers or biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects confidential and sensitive information.

We would welcome the opportunity to work with interested stakeholders to improve the bill.

Contact: Pete Isberg, Vice President, Government Relations, ADP, Inc. 909 971-7670
Pete.Isberg@adp.com

Specific Concerns for MD HB 259 - Biometric Identifiers Privacy

In addition to general concerns expressed separately, there are questions on various provisions in the bill. Because a private right of action is sought, it will be necessary to be extremely clear and comprehensive as to each element. Certain sections from the bill follow, with initial concerns explained in *red italics*.

14-4401

(G) "WRITTEN CONSENT' MEANS: (1) A SPECIFIC, DISCRETE, FREELY GIVEN, UNAMBIGUOUS, AND INFORMED CONSENT IN WRITING GIVEN BY AN INDIVIDUAL WHO IS NOT UNDER ANY DURESS OR UNDUE INFLUENCE FROM THE PRIVATE ENTITY OR THIRD PARTY TO WHOM THE CONSENT IS GIVEN AT THE TIME THE CONSENT IS GIVEN; OR (2) IN THE CONTEXT OF EMPLOYMENT, A RELEASE EXECUTED BY AN EMPLOYEE AS A CONDITION OF EMPLOYMENT.

Section 14.4401 requires "written consent" regardless of the type of interaction between an individual and private entity. As technology evolves, certain biometric uses do not allow for written consent to be readily obtained, such as the creation of voiceprints, used for security and fraud reduction purposes to authenticate callers. In such situations, verbal consent should be an alternative available for individuals.

14-4402

A) (1) EXCEPT AS PROVIDED IN SUBSECTION (B) OF THIS SECTION, EACH PRIVATE ENTITY IN POSSESSION OF BIOMETRIC IDENTIFIERS SHALL DEVELOP A WRITTEN POLICY, MADE AVAILABLE TO THE PUBLIC, ESTABLISHING A RETENTION SCHEDULE AND GUIDELINES FOR PERMANENTLY DESTROYING BIOMETRIC IDENTIFIERS ON THE EARLIEST OF THE FOLLOWING:

(I) THE DATE ON WHICH THE INITIAL PURPOSE FOR COLLECTING OR OBTAINING THE BIOMETRIC IDENTIFIERS HAS BEEN SATISFIED;
(II) WITHIN 1 YEAR AFTER THE INDIVIDUAL'S LAST INTERACTION WITH THE PRIVATE ENTITY IN POSSESSION OF THE BIOMETRIC IDENTIFIERS; OR
(III) WITHIN 30 DAYS AFTER THE PRIVATE ENTITY RECEIVES A VERIFIED REQUEST TO DELETE THE BIOMETRIC IDENTIFIERS SUBMITTED BY THE INDIVIDUAL OR THE INDIVIDUAL'S REPRESENTATIVE.

1. *Section 14.4402 (III) conflicts with the 14.4401(G)(2), which provides that "in the context of employment, [written consent means] a release executed by an employee as a condition of employment." Section 14.4402 (III) would permit employers to require employees to use appropriate biometric authentication systems, e.g., for security access controls, but then enable employees to immediately demand deletion, even before the purpose for which such biometric identifiers were collected has been satisfied. For example, timecards may need to be signed or otherwise acknowledged to be the official time record in order to have validity under state law. Deletion of such a signature may render critical employment records unusable.*

2. *14.4402(I) May also cause conflicts: "THE DATE ON WHICH THE INITIAL PURPOSE FOR COLLECTING OR OBTAINING THE BIOMETRIC IDENTIFIERS HAS BEEN SATISFIED;" A private entity may collect information for multiple purposes. This section would require deletion of the information after the first use of such information, rendering*

the entity unable to perform other intended purposes (or creating unintended legal liability).

3. *14.4402(II) this section was shortened from 3 years in previous proposals and now requires deletion after 1 year from an individual's last interaction with the private entity in possession of the biometric identifier. This could result in difficulty in the employment sector where biometric identifiers may be stored for security and timekeeping purposes, but used infrequently by certain employees, such as those who regularly work remotely or at a different worksite.*

14–4403.

AT THE REQUEST OF AN INDIVIDUAL OR AN INDIVIDUAL'S LEGALLY AUTHORIZED REPRESENTATIVE, A PRIVATE ENTITY THAT COLLECTS, USES, SHARES, OR SELLS BIOMETRIC IDENTIFIERS SHALL DISCLOSE, FREE OF CHARGE, THE BIOMETRIC IDENTIFIER AND INFORMATION RELATED TO THE USE OF THE BIOMETRIC IDENTIFIER TO THE INDIVIDUAL, INCLUDING:
(1) THE CATEGORIES OF BIOMETRIC IDENTIFIERS;
(2) SPECIFIC PIECES OF PERSONAL INFORMATION RELATED TO THE BIOMETRIC IDENTIFIERS;
(3) THE CATEGORIES OF SOURCES THAT THE PRIVATE ENTITY COLLECTED PERSONAL INFORMATION FROM LINKED TO THE BIOMETRIC IDENTIFIER;
(4) THE PURPOSES FOR WHICH THE PRIVATE ENTITY USED THE BIOMETRIC IDENTIFIER AND PERSONAL INFORMATION;
(5) **THE CATEGORIES OF THIRD PARTIES WITH WHOM THE PRIVATE ENTITY SHARES THE PERSONAL INFORMATION AND THE PURPOSES OF SHARING THE PERSONAL INFORMATION**; AND
(6) THE CATEGORIES OF INFORMATION THAT THE BUSINESS SELLS OR DISCLOSES TO THIRD PARTIES.

"Specific pieces of personal information related to the biometric identifiers" could be exhaustive, i.e., all data on file with respect to an employee who was authenticated through biometric information, e.g.,

- *For a retail worker, details of every routine transaction completed by the employee for which the employee was authenticated using biometric information*
- *For an office worker, details of every routine written communication ever sent or received through a system for which the employee was authenticated using biometric information*

14.4403(5) and (6) above may require disclosure and explanations of routine data transfers to processors such as payroll service providers, retirement plan administrators, and even between payroll processors and third-party data storage service providers, as well as reporting required by various government agencies, such as employer reporting of newly-hired employees or contractors to child support agencies, reporting of wages to the unemployment insurance agency; reports of wages and withholding to the tax authorities and so on.

This uncertainty and lack of definition coupled with the private right of action would lead to a flood of lawsuits challenging businesses' disclosures under this section as inadequate, incomplete or

insufficiently detailed. If a private right of action is thought to be necessary, any information required to be disclosed should be spelled out thoroughly and comprehensively.

14–4404.
(A) A PRIVATE ENTITY THAT COLLECTS BIOMETRIC IDENTIFIERS MAY NOT SELL, LEASE, TRADE, OR OTHERWISE PROFIT FROM AN INDIVIDUAL'S BIOMETRIC IDENTIFIERS.

"Otherwise profit" may conflict with all private sector operations. Arguably all private entities could be said to "profit" from the use of biometric systems by reducing fraud and improving security.

(B) A PRIVATE ENTITY THAT COLLECTS BIOMETRIC IDENTIFIERS MAY NOT COLLECT, USE, DISCLOSE, REDISCLOSE, OR OTHERWISE DISSEMINATE AN INDIVIDUAL'S BIOMETRIC IDENTIFIERS UNLESS:

(1) THE INDIVIDUAL OR THE INDIVIDUAL'S LEGALLY AUTHORIZED REPRESENTATIVE PROVIDES WRITTEN CONSENT TO THE PARTICULAR OR CATEGORY OF COLLECTION, USE DISCLOSURE, REDISCLOSURE, OR DISSEMINATION; OR
(2) THE DISCLOSURE OR REDISCLOSURE IS REQUIRED BY A VALID WARRANT OR SUBPOENA.

In the context of employment, Section 14-4404 (B) could require employers to seek each employee's consent to transfer data to a payroll service provider, which by charging the employer fees for such services could be said to profit from the collection, storage and/or processing of such information. It would be impractical to seek express written consent from each employee to permit payroll administration.

A requirement for written consent may effectively prevent Maryland employers from using any form of voice recognition systems, which are an increasingly effective and important means of authentication, which serves to improve workplace safety, security and integrity, and reduce fraud.

(D) (1) A PRIVATE ENTITY THAT CONTRACTS WITH A PROCESSOR TO PROCESS OR STORE BIOMETRIC IDENTIFIERS MAY NOT ALLOW THE PROCESSOR TO COLLECT, STORE, PROCESS, USE, DISCLOSE, OR CONDUCT ANY ACTION FOR PROFIT OR OTHERWISE ON OR WITH THE BIOMETRIC IDENTIFIERS EXCEPT FOR PURPOSES FOR WHICH THE PRIVATE ENTITY RECEIVED EXPRESS WRITTEN CONSENT FROM THE INDIVIDUAL.

It is not clear whether or how the exclusion expressed in Sec. 14-4401 E. (2) (IV) would apply and interact with this section:

> *14-4401 E. (2) "PRIVATE ENTITY" DOES NOT INCLUDE:*
> *(IV) AN ENTITY ACTING AS A PROCESSOR FOR ANOTHER ENTITY.*
>
> *(F) (1) "PROCESSOR" MEANS AN ENTITY THAT PROCESSES, STORES, OR OTHERWISE USES BIOMETRIC IDENTIFIERS ON BEHALF OF A PRIVATE ENTITY*

Otherwise, in the context of employment, this clause could prohibit employers from using a payroll service provider, which by charging the employer fees for such services could be said to profit from the collection, storage and/or processing of such information. Again, it would be impractical to seek express written consent from each employee to permit payroll administration.

(2) A PROCESSOR MAY NOT COLLECT, STORE, PROCESS, USE, DISCLOSE, OR CONDUCT ANY ACTION FOR PROFIT OR OTHERWISE ON OR WITH BIOMETRIC IDENTIFIERS, EXCEPT AS AUTHORIZED BY A CONTRACT WITH A PRIVATE ENTITY THAT LEGALLY POSSESSES THE BIOMETRIC IDENTIFIERS.

It may be impractical or impossible for processors to affirmatively and continuously confirm that a private entity client legally possesses biometric identifiers. For example, a payroll processor would not necessarily know when the legal basis for processing has ended, e.g., the employer must tell their processor when an employee no longer needs to use a timeclock, for example because they transferred, work remotely, or moved to a salaried position.

It is not clear what is intended by the "on or with" clause in "A processor may not collect, store, process, use, disclose, or conduct any action …on or with biometric identifiers." Plaintiffs' attorneys could seek to extend the prohibition to all employment-related data generated after authentication by a biometric identifier.

Further, some contracts may not specifically authorize every potential disclosure of employment-related data generated after authentication by a biometric identifier, such as those required by law.

14–4405.
(A) AN INDIVIDUAL ALLEGING A VIOLATION OF THIS SUBTITLE MAY BRING A CIVIL ACTION AGAINST THE OFFENDING PRIVATE ENTITY.
(B) AN INDIVIDUAL WHO PREVAILS IN A CIVIL ACTION UNDER THIS SECTION MAY RECOVER FOR EACH VIOLATION:
(1) AGAINST A PRIVATE ENTITY THAT NEGLIGENTLY VIOLATED A PROVISION OF THIS SUBTITLE, $1,000 OR ACTUAL DAMAGES, WHICHEVER IS GREATER;
(2) AGAINST A PRIVATE ENTITY THAT INTENTIONALLY OR RECKLESSLY VIOLATED A PROVISION OF THIS SUBTITLE, $5,000 OR ACTUAL DAMAGES, WHICHEVER IS GREATER;
(3) REASONABLE ATTORNEY'S FEES AND COSTS, INCLUDING EXPERT WITNESS FEES AND OTHER LITIGATION EXPENSES; AND
(4) OTHER RELIEF, INCLUDING AN INJUNCTION, AS THE COURT MAY DETERMINE APPROPRIATE.

In the context of employment, "each violation" may translate to an astronomical damage award, given that any violation may be deemed to be a separate violation for every transaction conducted by each employee of en employer over the course of multiple years. A similar law in Illinois enabled plaintiffs' attorneys to threaten lawsuits seeking billions of dollars in damages.