SENATE BILL 973

D3 3lr2931

By: **Senators Simonaire, Hester, and Jennings**
Introduced and read first time: February 28, 2023
Assigned to: Rules

A BILL ENTITLED

AN ACT concerning

Civil Actions – Affirmative Defenses – Business Data Breaches

FOR the purpose of establishing an affirmative defense to a civil action arising out of certain data breaches; establishing certain requirements for a covered business entity seeking to assert the affirmative defense established under this Act; providing that this Act may not be construed to create a private right of action or to affect any other immunity or defense available under statute or the common law; and generally relating to affirmative defenses and data breaches.

BY adding to
Article – Courts and Judicial Proceedings
Section 5–1301 through 5–1304 to be under the new subtitle "Subtitle 13. Affirmative Defenses – Data Breaches"
Annotated Code of Maryland
(2020 Replacement Volume and 2022 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Courts and Judicial Proceedings

SUBTITLE 13. AFFIRMATIVE DEFENSES – DATA BREACHES.

5–1301.

(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVING THE MEANINGS INDICATED.

(B) (1) "COVERED ENTITY" MEANS A PRIVATE FOR–PROFIT OR NONPROFIT BUSINESS ENTITY THAT ACCESSES, MAINTAINS, COMMUNICATES, OR

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

PROCESSES PERSONAL INFORMATION OR RESTRICTED INFORMATION IN OR THROUGH ONE OR MORE SYSTEMS, NETWORKS, OR SERVICES LOCATED IN OR OUTSIDE THE STATE.

(2) "COVERED ENTITY" INCLUDES A FINANCIAL INSTITUTION ORGANIZED, CHARTERED, LICENSED, OR OTHERWISE AUTHORIZED UNDER THE LAWS OF THE STATE, ANY OTHER STATE, THE UNITED STATES, OR ANY OTHER COUNTRY, OR THE PARENT OR SUBSIDIARY OF A FINANCIAL INSTITUTION.

(3) "COVERED ENTITY" DOES NOT INCLUDE A UNIT OF STATE OR LOCAL GOVERNMENT.

(C) (1) "DATA BREACH" MEANS THE UNAUTHORIZED ACCESS TO, AND ACQUISITION OF, COMPUTERIZED DATA THAT COMPROMISES THE SECURITY OR CONFIDENTIALITY OF PERSONAL INFORMATION OR RESTRICTED INFORMATION OWNED BY OR LICENSED TO A COVERED ENTITY THAT CAUSES, IS REASONABLY BELIEVED TO HAVE CAUSED, OR IS REASONABLY BELIEVED WILL CAUSE A MATERIAL RISK OF IDENTITY THEFT OR OTHER FRAUD TO PERSON OR PROPERTY.

(2) "DATA BREACH" DOES NOT INCLUDE:

(I) A GOOD FAITH ACQUISITION OF PERSONAL INFORMATION OR RESTRICTED INFORMATION BY AN EMPLOYEE OR AGENT OF A COVERED ENTITY FOR A LEGITIMATE PURPOSE, PROVIDED THAT THE PERSONAL INFORMATION OR RESTRICTED INFORMATION IS NOT SUBJECT TO UNAUTHORIZED DISCLOSURE; OR

(II) AN ACQUISITION OF PERSONAL INFORMATION OR RESTRICTED INFORMATION IN ACCORDANCE WITH A SEARCH WARRANT, SUBPOENA, OR OTHER LAWFUL ORDER.

(D) (1) "PERSONAL INFORMATION" MEANS AN INDIVIDUAL'S FIRST NAME AND LAST NAME OR FIRST INITIAL AND LAST NAME, PERSONAL MARK, OR UNIQUE BIOMETRIC OR GENETIC PRINT OR IMAGE, IN COMBINATION WITH ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT ARE NOT ENCRYPTED, REDACTED, OR SIMILARLY UNREADABLE:

(I) A SOCIAL SECURITY NUMBER;

(II) A DRIVER'S LICENSE NUMBER, STATE IDENTIFICATION CARD NUMBER, OR OTHER INDIVIDUAL IDENTIFICATION NUMBER ISSUED BY A UNIT OF STATE OR LOCAL GOVERNMENT;

(III) A PASSPORT NUMBER OR OTHER IDENTIFICATION NUMBER ISSUED BY THE FEDERAL GOVERNMENT;

(IV) AN INDIVIDUAL TAXPAYER IDENTIFICATION NUMBER; OR

(V) A FINANCIAL OR OTHER ACCOUNT NUMBER, A CREDIT CARD NUMBER, OR A DEBIT CARD NUMBER THAT, IN COMBINATION WITH ANY REQUIRED SECURITY CODE, ACCESS CODE, OR PASSWORD, WOULD PERMIT ACCESS TO AN INDIVIDUAL'S ACCOUNT.

(2) "PERSONAL INFORMATION" DOES NOT INCLUDE:

(I) A VOTER REGISTRATION NUMBER;

(II) INFORMATION THAT IS LAWFULLY MADE PUBLICLY AVAILABLE FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS;

(III) INFORMATION THAT AN INDIVIDUAL HAS CONSENTED TO HAVE PUBLICLY DISSEMINATED OR LISTED; OR

(IV) INFORMATION THAT IS WIDELY DISTRIBUTED OR PUBLISHED.

(E) "RESTRICTED INFORMATION" MEANS INFORMATION REGARDING AN INDIVIDUAL, OTHER THAN PERSONAL INFORMATION, THAT ALONE OR IN COMBINATION WITH OTHER INFORMATION, INCLUDING PERSONAL INFORMATION, CAN BE USED TO DISTINGUISH OR TRACE THE IDENTITY OF AN INDIVIDUAL OR THAT IS LINKED OR LINKABLE TO AN INDIVIDUAL IF:

(1) THE INFORMATION IS NOT ENCRYPTED, REDACTED, OR SIMILARLY UNREADABLE; AND

(2) THE BREACH OF WHICH IS LIKELY TO RESULT IN A MATERIAL RISK OF IDENTITY THEFT OR OTHER FRAUD TO PERSON OR PROPERTY.

5–1302.

(A) A COVERED ENTITY MAY ASSERT AN AFFIRMATIVE DEFENSE AGAINST A CLAIM ARISING OUT OF A DATA BREACH INVOLVING PERSONAL INFORMATION OR RESTRICTED INFORMATION IF, AT THE TIME OF THE DATA BREACH GIVING RISE TO THE CLAIM, THE COVERED ENTITY HAD, MAINTAINED, AND COMPLIED WITH A WRITTEN CYBERSECURITY PROGRAM THAT:

(1) CONTAINED ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS THAT REASONABLY CONFORM TO AN INDUSTRY–RECOGNIZED CYBERSECURITY FRAMEWORK DESCRIBED UNDER § 5–1303 OF THIS SUBTITLE;

(2) MET THE APPLICABLE REQUIREMENTS OF SUBSECTION (B) OF THIS SECTION; AND

(3) PROVIDED FOR THE PROTECTION OF PERSONAL INFORMATION AND RESTRICTED INFORMATION, AS APPLICABLE.

(B) (1) A COVERED ENTITY INVOKING AN AFFIRMATIVE DEFENSE UNDER SUBSECTION (A) OF THIS SECTION AGAINST A CLAIM ARISING OUT OF A DATA BREACH SHALL DEMONSTRATE THAT THE CYBERSECURITY PROGRAM OF THE COVERED ENTITY WAS APPROPRIATE IN SCALE AND SCOPE TO PROTECT AGAINST:

(I) ANTICIPATED THREATS OR HAZARDS TO THE SECURITY OR INTEGRITY OF THE INFORMATION; AND

(II) UNAUTHORIZED ACCESS TO AND ACQUISITION OF THE INFORMATION LIKELY TO RESULT IN A MATERIAL RISK OF IDENTITY THEFT OR OTHER FRAUD TO THE INDIVIDUAL TO WHOM THE INFORMATION RELATED.

(2) THE FOLLOWING FACTORS SHALL BE CONSIDERED BY THE COURT IN DETERMINING WHETHER THE CYBERSECURITY PROGRAM OF THE COVERED ENTITY WAS OF AN APPROPRIATE SCALE AND SCOPE:

(I) THE SIZE AND COMPLEXITY OF THE COVERED ENTITY;

(II) THE NATURE AND SCOPE OF THE ACTIVITIES OF THE COVERED ENTITY;

(III) THE SENSITIVITY AND TYPE OF INFORMATION BEING PROTECTED;

(IV) THE COST AND AVAILABILITY OF TOOLS TO IMPROVE INFORMATION SECURITY AND REDUCE VULNERABILITIES; AND

(V) THE RESOURCES AVAILABLE TO THE COVERED ENTITY.

5–1303.

THE CYBERSECURITY PROGRAM OF A COVERED ENTITY SHALL BE DEEMED TO HAVE REASONABLY CONFORMED TO AN INDUSTRY–RECOGNIZED CYBERSECURITY

FRAMEWORK OR STANDARD FOR THE PURPOSE OF INVOKING AN AFFIRMATIVE DEFENSE UNDER § 5–1302 OF THIS SUBTITLE IF, BASED ON THE TYPE OF DATA BEING PROTECTED, THE CYBERSECURITY PROGRAM REASONABLY CONFORMED TO THE VERSION OF ANY OF THE FOLLOWING EFFECTIVE AT THE TIME OF, OR WITHIN 1 YEAR BEFORE, THE DATA BREACH:

(1) (I) 1. THE FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY DEVELOPED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY;

2. SPECIAL PUBLICATION 800–171 OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY;

3. SPECIAL PUBLICATIONS 800–53 AND 800–53A OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY;

4. THE SECURITY ASSESSMENT FRAMEWORK FOR THE FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM, ALSO KNOWN AS FEDRAMP;

5. THE CENTER FOR INTERNET SECURITY CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE, PUBLISHED BY THE CENTER FOR INTERNET SECURITY; OR

6. THE 27000–SERIES INFORMATION SECURITY MANAGEMENT SYSTEMS, ESTABLISHED BY THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND THE INTERNATIONAL ELECTROTECHNICAL COMMISSION; AND

(II) IF APPLICABLE, THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD, AS ESTABLISHED BY THE PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL; OR

(2) (I) THE SECURITY REQUIREMENTS OF THE FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, AS SET FORTH IN 45 C.F.R. PART 164, SUBPART C;

(II) TITLE V OF THE FEDERAL GRAMM–LEACH–BLILEY ACT OF 1999;

(III) THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014; OR

(IV) THE FEDERAL HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT, AS SET FORTH IN 45 C.F.R. PART 162.

5–1304.

THIS SUBTITLE MAY NOT BE CONSTRUED TO:

(1) CREATE A PRIVATE RIGHT OF ACTION, INCLUDING A CLASS ACTION, WITH RESPECT TO ANY ACT OR PRACTICE DESCRIBED UNDER THIS SUBTITLE; OR

(2) AFFECT ANY OTHER IMMUNITY FROM CIVIL LIABILITY OR DEFENSE ESTABLISHED BY ANY OTHER PROVISION OF LAW OR AVAILABLE AT COMMON LAW, TO WHICH A COVERED ENTITY MAY BE ENTITLED.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall be construed to apply only prospectively and may not be applied or interpreted to have any effect on or application to any cause of action arising before the effective date of this Act.

SECTION 3. AND BE IT FURTHER ENACTED, That, if any provision of this Act or the application thereof to any person or circumstance is held invalid for any reason in a court of competent jurisdiction, the invalidity does not affect other provisions or any other application of this Act that can be given effect without the invalid provision or application, and for this purpose the provisions of this Act are declared severable.

SECTION 4. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2023.