SENATE BILL 194

I3, P1 7lr1670
SB 134/06 – FIN CF HB 208

By: **Senators Kelley, Astle, Garagiola, Klausmeier, and Middleton**
Introduced and read first time: January 26, 2007
Assigned to: Finance

A BILL ENTITLED

AN ACT concerning

Consumer Protection – Personal Information Protection Act

FOR the purpose of requiring a certain business, when destroying a customer's records that contain certain personal information of the customer, to take certain steps to protect against unauthorized access to or use of the personal information under certain circumstances; requiring a certain business that owns or licenses certain personal information of an individual residing in the State to implement and maintain certain security procedures and practices under certain circumstances; requiring certain businesses that own, license, or maintain computerized data that includes certain personal information of an individual residing in the State to conduct a certain investigation and notify certain persons of a breach of the security of a system under certain circumstances; specifying the time at which notification must be given; authorizing notification to be given in a certain manner; providing that a waiver of certain provisions of this Act is contrary to public policy and is void and unenforceable; providing that compliance with certain provisions of this Act does not relieve a certain business from a duty to comply with certain other requirements of federal law; providing that the provisions of this Act are exclusive and shall preempt any provision of local law; requiring a business to report to certain consumer reporting agencies on the breach of the security of a system under certain circumstances; providing that certain businesses and affiliates shall be deemed to be in compliance with the requirements of this Act under certain circumstances; providing that a violation of this Act is an unfair or deceptive trade practice within the meaning of the Maryland Consumer Protection Act and is subject to certain enforcement and penalty provisions; defining certain terms; providing for a delayed effective date; and generally relating to the

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

protection of personal information contained in the records of businesses, owned or licensed by businesses, or included in computerized data owned, licensed, or maintained by businesses.

BY adding to
Article – Commercial Law
Section 14–3501 through 14–3508 to be under the new subtitle "Subtitle 35. Maryland Personal Information Protection Act"
Annotated Code of Maryland
(2005 Replacement Volume and 2006 Supplement)

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

Article – Commercial Law

SUBTITLE 35. MARYLAND PERSONAL INFORMATION PROTECTION ACT.

14–3501.

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

(B) (1) "BUSINESS" MEANS A SOLE PROPRIETORSHIP, PARTNERSHIP, CORPORATION, ASSOCIATION, OR ANY OTHER BUSINESS ENTITY, WHETHER OR NOT ORGANIZED TO OPERATE AT A PROFIT.

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

(3) "BUSINESS" DOES NOT INCLUDE AN ENTITY THAT HAS AN ANNUAL GROSS INCOME OF LESS THAN $1,000,000.

(C) (1) "PERSONAL INFORMATION" MEANS AN INDIVIDUAL'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS, WHEN THE NAME OR THE DATA ELEMENTS ARE NOT ENCRYPTED, REDACTED, OR OTHERWISE PROTECTED BY ANOTHER METHOD THAT RENDERS THE INFORMATION UNREADABLE OR UNUSABLE:

(I) A SOCIAL SECURITY NUMBER;

(II) A DRIVER'S LICENSE NUMBER;

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

(IV) A CONSUMER REPORT, AS DEFINED IN § 14–1201 OF THIS TITLE.

(2) "PERSONAL INFORMATION" DOES NOT INCLUDE:

(I) PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS;

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

(III) INFORMATION THAT IS DISSEMINATED OR LISTED IN ACCORDANCE WITH THE FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT.

(D) "RECORDS" MEANS INFORMATION THAT IS INSCRIBED ON A TANGIBLE MEDIUM OR THAT IS STORED IN AN ELECTRONIC OR OTHER MEDIUM AND IS RETRIEVABLE IN PERCEIVABLE FORM.

14–3502.

(A) IN THIS SECTION, "CUSTOMER" MEANS AN INDIVIDUAL RESIDING IN THE STATE WHO PROVIDES PERSONAL INFORMATION TO A BUSINESS FOR THE PURPOSE OF PURCHASING OR LEASING A PRODUCT OR OBTAINING A SERVICE FROM THE BUSINESS.

(B) WHEN A BUSINESS IS DESTROYING A CUSTOMER'S RECORDS THAT CONTAIN PERSONAL INFORMATION OF THE CUSTOMER, THE BUSINESS SHALL

TAKE REASONABLE STEPS TO PROTECT AGAINST UNAUTHORIZED ACCESS TO OR USE OF THE PERSONAL INFORMATION, TAKING INTO ACCOUNT:

(1) THE SENSITIVITY OF THE RECORDS;

(2) THE NATURE AND SIZE OF THE BUSINESS AND ITS OPERATIONS;

(3) THE COSTS AND BENEFITS OF DIFFERENT DESTRUCTION METHODS; AND

(4) AVAILABLE TECHNOLOGY.

14–3503.

(A) TO PROTECT PERSONAL INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, OR DISCLOSURE, A BUSINESS THAT OWNS OR LICENSES PERSONAL INFORMATION OF AN INDIVIDUAL RESIDING IN THE STATE SHALL IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE NATURE OF THE PERSONAL INFORMATION OWNED OR LICENSED AND THE NATURE AND SIZE OF THE BUSINESS AND ITS OPERATIONS.

(B) (1) A BUSINESS THAT USES A NONAFFILIATED THIRD PARTY AS A SERVICE PROVIDER TO PERFORM SERVICES FOR THE BUSINESS AND DISCLOSES PERSONAL INFORMATION ABOUT AN INDIVIDUAL RESIDING IN THE STATE UNDER A WRITTEN CONTRACT WITH THE THIRD PARTY SHALL REQUIRE BY CONTRACT THAT THE THIRD PARTY IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT:

(I) ARE APPROPRIATE TO THE NATURE OF THE PERSONAL INFORMATION DISCLOSED TO THE NONAFFILIATED THIRD PARTY; AND

(II) ARE REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION.

(2) THIS SUBSECTION SHALL APPLY TO A WRITTEN CONTRACT THAT IS ENTERED INTO ON OR AFTER JANUARY 1, 2009.

14–3504.

(A) IN THIS SECTION:

(1) "BREACH OF THE SECURITY OF A SYSTEM" MEANS THE UNAUTHORIZED ACQUISITION OF COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF THE PERSONAL INFORMATION MAINTAINED BY A BUSINESS AND WILL LIKELY RESULT IN A MATERIAL RISK OF IDENTITY THEFT; AND

(2) "BREACH OF THE SECURITY OF A SYSTEM" DOES NOT INCLUDE THE GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A BUSINESS FOR THE PURPOSES OF THE BUSINESS, PROVIDED THAT:

(I) THE PERSONAL INFORMATION IS NOT USED OR SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE; AND

(II) IT IS NOT LIKELY THAT THE ACQUISITION WILL RESULT IN A MATERIAL RISK OF IDENTITY THEFT.

(B) (1) A BUSINESS THAT OWNS OR LICENSES COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION OF AN INDIVIDUAL RESIDING IN THE STATE, WHEN IT DISCOVERS OR IS NOTIFIED OF A BREACH OF THE SECURITY OF A SYSTEM, SHALL CONDUCT IN GOOD FAITH A REASONABLE AND PROMPT INVESTIGATION TO DETERMINE THE LIKELIHOOD THAT THE BREACH WILL RESULT IN A MATERIAL RISK OF IDENTITY THEFT.

(2) IF, AFTER THE INVESTIGATION IS CONCLUDED, THE BUSINESS REASONABLY BELIEVES THAT THE BREACH OF THE SECURITY OF A SYSTEM HAS RESULTED OR WILL RESULT IN A MATERIAL RISK OF IDENTITY THEFT OF PERSONAL INFORMATION OF AN INDIVIDUAL RESIDING IN THE STATE, THE BUSINESS SHALL NOTIFY THE INDIVIDUAL OF THE BREACH.

(3) EXCEPT AS PROVIDED IN SUBSECTION (D) OF THIS SECTION, THE NOTIFICATION REQUIRED UNDER PARAGRAPH (2) OF THIS SUBSECTION SHALL BE GIVEN AS SOON AS REASONABLY PRACTICABLE AFTER THE BUSINESS

CONDUCTS THE INVESTIGATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION.

(C) (1) A BUSINESS THAT MAINTAINS COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION THAT THE BUSINESS DOES NOT OWN OR LICENSE SHALL NOTIFY THE OWNER OR LICENSEE OF THE PERSONAL INFORMATION OF A BREACH OF THE SECURITY OF A SYSTEM IF IT IS LIKELY THAT THE BREACH HAS RESULTED OR WILL RESULT IN A MATERIAL RISK OF IDENTITY THEFT OF PERSONAL INFORMATION OF AN INDIVIDUAL RESIDING IN THE STATE.

(2) EXCEPT AS PROVIDED IN SUBSECTION (D) OF THIS SECTION, THE NOTIFICATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL BE GIVEN AS SOON AS REASONABLY PRACTICABLE AFTER THE BUSINESS DISCOVERS OR IS NOTIFIED OF THE BREACH OF THE SECURITY OF A SYSTEM.

(D) (1) THE NOTIFICATION REQUIRED UNDER SUBSECTIONS (B) AND (C) OF THIS SECTION MAY BE DELAYED:

(I) IF A LAW ENFORCEMENT AGENCY DETERMINES THAT THE NOTIFICATION WILL IMPEDE A CRIMINAL INVESTIGATION OR JEOPARDIZE HOMELAND OR NATIONAL SECURITY; OR

(II) TO DETERMINE THE SCOPE OF THE BREACH OF THE SECURITY OF A SYSTEM, IDENTIFY THE INDIVIDUALS AFFECTED, OR RESTORE THE INTEGRITY OF THE SYSTEM.

(2) IF NOTIFICATION IS DELAYED UNDER PARAGRAPH (1)(I) OF THIS SUBSECTION, NOTIFICATION SHALL BE GIVEN AS SOON AS REASONABLY PRACTICABLE AFTER THE LAW ENFORCEMENT AGENCY DETERMINES THAT IT WILL NOT IMPEDE A CRIMINAL INVESTIGATION AND WILL NOT JEOPARDIZE HOMELAND OR NATIONAL SECURITY.

(E) THE NOTIFICATION REQUIRED UNDER SUBSECTIONS (B) AND (C) OF THIS SECTION MAY BE GIVEN:

(1) BY WRITTEN NOTICE SENT TO THE MOST RECENT ADDRESS OF THE INDIVIDUAL IN THE RECORDS OF THE BUSINESS;

(2) BY ELECTRONIC NOTICE, IF THE ELECTRONIC NOTICE IS CONSISTENT WITH THE REQUIREMENTS FOR ELECTRONIC RECORDS AND SIGNATURES UNDER 15 U.S.C. § 7001;

(3) BY TELEPHONIC NOTICE, TO THE MOST RECENT TELEPHONE NUMBER OF THE INDIVIDUAL IN THE RECORDS OF THE BUSINESS; OR

(4) BY SUBSTITUTE NOTICE AS PROVIDED IN SUBSECTION (F) OF THIS SECTION, IF:

(I) THE BUSINESS DEMONSTRATES THAT THE COST OF PROVIDING NOTICE WOULD EXCEED $25,000 OR THAT THE AFFECTED CLASS OF INDIVIDUALS TO BE NOTIFIED EXCEEDS 50,000; OR

(II) THE BUSINESS DOES NOT HAVE SUFFICIENT CONTACT INFORMATION TO GIVE NOTICE IN ACCORDANCE WITH ITEM (1), (2), OR (3) OF THIS SUBSECTION.

(F) SUBSTITUTE NOTICE UNDER SUBSECTION (E)(4) OF THIS SECTION SHALL CONSIST OF:

(1) ELECTRONICALLY MAILING THE NOTICE TO AN INDIVIDUAL ENTITLED TO NOTIFICATION UNDER SUBSECTION (B) OF THIS SECTION, IF THE BUSINESS HAS AN ELECTRONIC MAIL ADDRESS FOR THE INDIVIDUAL TO BE NOTIFIED;

(2) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE OF THE BUSINESS, IF THE BUSINESS MAINTAINS A WEBSITE; AND

(3) NOTIFICATION TO STATEWIDE MEDIA.

(G) A BUSINESS SHALL PROVIDE NOTICE OF A BREACH OF THE SECURITY OF A SYSTEM TO THE OFFICE OF THE ATTORNEY GENERAL WITHIN 5 BUSINESS DAYS AFTER THE BUSINESS BECOMES AWARE OF THE BREACH.

(H) A WAIVER OF ANY PROVISION OF THIS SECTION IS CONTRARY TO PUBLIC POLICY AND IS VOID AND UNENFORCEABLE.

(I) COMPLIANCE WITH THIS SECTION DOES NOT RELIEVE A BUSINESS FROM A DUTY TO COMPLY WITH ANY OTHER REQUIREMENTS OF FEDERAL LAW RELATING TO THE PROTECTION AND PRIVACY OF PERSONAL INFORMATION.

14–3505.

THE PROVISIONS OF THIS SUBTITLE ARE EXCLUSIVE AND SHALL PREEMPT ANY PROVISION OF LOCAL LAW.

14–3506.

(A) IF A BUSINESS IS REQUIRED UNDER § 14–3504 OF THIS SUBTITLE TO GIVE NOTICE OF A BREACH OF THE SECURITY OF A SYSTEM TO 1,000 OR MORE INDIVIDUALS, THE BUSINESS ALSO SHALL NOTIFY, WITHOUT UNREASONABLE DELAY, EACH CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED BY 15 U.S.C. § 1681A(P), OF THE TIMING, DISTRIBUTION, AND CONTENT OF THE NOTICES.

(B) THIS SECTION DOES NOT REQUIRE THE INCLUSION OF THE NAMES OR OTHER PERSONAL IDENTIFYING INFORMATION OF RECIPIENTS OF NOTICES OF THE BREACH OF THE SECURITY OF A SYSTEM.

14–3507.

(A) IN THIS SECTION, "AFFILIATE" MEANS A COMPANY THAT CONTROLS, IS CONTROLLED BY, OR IS UNDER COMMON CONTROL WITH A BUSINESS DESCRIBED IN SUBSECTION (C)(1) OF THIS SECTION.

(B) A BUSINESS THAT COMPLIES WITH THE REQUIREMENTS FOR NOTIFICATION PROCEDURES, THE PROTECTION OR SECURITY OF PERSONAL INFORMATION, OR THE DESTRUCTION OF PERSONAL INFORMATION UNDER THE RULES, REGULATIONS, PROCEDURES, OR GUIDELINES ESTABLISHED BY THE PRIMARY OR FUNCTIONAL FEDERAL OR STATE REGULATOR OF THE BUSINESS SHALL BE DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.

(C) (1) A BUSINESS THAT IS SUBJECT TO AND IN COMPLIANCE WITH § 501(B) OF THE FEDERAL GRAMM–LEACH–BLILEY ACT, 15 U.S.C. § 6801, § 216 OF THE FEDERAL FAIR AND ACCURATE TRANSACTIONS ACT, 15 U.S.C. § 1681W, THE FEDERAL INTERAGENCY GUIDELINES ESTABLISHING

INFORMATION SECURITY STANDARDS, AND THE FEDERAL INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE, AND ANY REVISIONS, ADDITIONS, OR SUBSTITUTIONS, SHALL BE DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.

(2) AN AFFILIATE THAT COMPLIES WITH § 501(B) OF THE FEDERAL GRAMM–LEACH–BLILEY ACT, 15 U.S.C. § 6801, § 216 OF THE FEDERAL FAIR AND ACCURATE TRANSACTIONS ACT, 15 U.S.C. § 1681W, THE FEDERAL INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS, AND THE FEDERAL INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE, AND ANY REVISIONS, ADDITIONS, OR SUBSTITUTIONS, SHALL BE DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.

14–3508.

A VIOLATION OF THIS SUBTITLE:

(1) IS AN UNFAIR OR DECEPTIVE TRADE PRACTICE WITHIN THE MEANING OF TITLE 13 OF THIS ARTICLE; AND

(2) IS SUBJECT TO THE ENFORCEMENT AND PENALTY PROVISIONS CONTAINED IN TITLE 13 OF THIS ARTICLE.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect January 1, 2008.