HB0716/204732/1

BY: Education, Health, and Environmental Affairs Committee

AMENDMENTS TO HOUSE BILL 716
(Third Reading File Bill)

AMENDMENT NO. 1

On page 1, in line 4, after the second "of" insert "the Executive Branch of"; in line 6, strike the second "certain"; in lines 6 and 7, strike "of State government"; strike beginning with "establishing" in line 22 down through "Maryland;" in line 23; and in line 24, strike "law" and substitute "this Act".

On pages 1 and 2, strike beginning with "repealing" in line 24 on page 1 down through "definitions;" in line 1 on page 2.

On page 2, in line 1, strike "the" and substitute "a delayed"; in the same line, strike "of certain" and substitute a semicolon; strike line 2 in its entirety; after line 4, insert:

"BY repealing and reenacting, without amendments,
Article - State Government
Section 10-1301(a)
Annotated Code of Maryland
(2014 Replacement Volume and 2018 Supplement)";

strike beginning with "10–1301" in line 7 down through "(j)" in line 8 and substitute "10–1301(f) and 10–1302(b) to be under the amended subtitle "Subtitle 13. Protection of Information by Public Institutions of Higher Education and Political Subdivisions""; in line 13, strike "10–13A–08" and substitute "10–13A–07"; in line 14, strike "University System of Maryland" and substitute "Executive Branch"; and strike in their entirety lines 17 through 22, inclusive.

AMENDMENT NO. 2

(Over)

On page 2, after line 25, insert:

"Subtitle 13. Protection of Information by **[**Government Agencies**]** **PUBLIC INSTITUTIONS OF HIGHER EDUCATION AND POLITICAL SUBDIVISIONS**.".

On pages 2 through 4, strike in their entirety the lines beginning with line 28 on page 2 through line 33 on page 4, inclusive.

On page 5, in line 1, strike the brackets; in the same line, strike "**(G)**"; strike beginning with "an" in line 2 down through "authority," in line 3; in line 3, strike ", a unit"; and strike in their entirety lines 9 through 29, inclusive.

On page 6, in line 1, strike the brackets; in the same line, strike "**(C)**" and substitute "**(1)**"; in the same line, after "to" insert "**:**

(I)";

strike beginning with the first comma in line 2 down through "**MARYLAND**" in line 3 and substitute "**; OR**

(II) EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS SUBSECTION, THE EXECUTIVE BRANCH OF STATE GOVERNMENT.

(2) THIS SUBTITLE APPLIES TO A PUBLIC INSTITUTION OF HIGHER EDUCATION AND AN INSTRUMENTALITY OF THE STATE";

and after line 3, insert:

"**SUBTITLE 13A. PROTECTION OF INFORMATION BY THE EXECUTIVE BRANCH.**

10–13A–01.

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

(B) "ENCRYPTION" MEANS THE PROTECTION OF DATA IN ELECTRONIC OR OPTICAL FORM, IN STORAGE OR IN TRANSIT, USING A TECHNOLOGY THAT:

(1) IS CERTIFIED TO MEET OR EXCEED THE LEVEL THAT HAS BEEN ADOPTED BY THE FEDERAL INFORMATION PROCESSING STANDARDS ISSUED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; AND

(2) RENDERS THE DATA INDECIPHERABLE WITHOUT AN ASSOCIATED CRYPTOGRAPHIC KEY NECESSARY TO ENABLE DECRYPTION OF THE DATA.

(C) "INDIVIDUAL" MEANS AN INDIVIDUAL WHO INTERACTS WITH A UNIT.

(D) (1) "PERSONALLY IDENTIFIABLE INFORMATION" MEANS INFORMATION THAT MAY BE USED TO DISTINGUISH OR TRACE AN INDIVIDUAL'S IDENTITY, EITHER ALONE OR WHEN COMBINED WITH OTHER INFORMATION ASSOCIATED WITH AN INDIVIDUAL.

(2) "PERSONALLY IDENTIFIABLE INFORMATION" INCLUDES:

(I) UNIQUE PERSONAL IDENTIFIERS, INCLUDING:

1. A FULL NAME;

2. A FIRST INITIAL AND LAST NAME;

3. A SOCIAL SECURITY NUMBER;

4. A DRIVER'S LICENSE NUMBER, A STATE IDENTIFICATION NUMBER, OR OTHER IDENTIFICATION NUMBER ISSUED BY A UNIT; AND

5. A PASSPORT NUMBER;

(II) CHARACTERISTICS OR CLASSIFICATIONS PROTECTED UNDER FEDERAL OR STATE LAW;

(III) BIOMETRIC INFORMATION INCLUDING AN INDIVIDUAL'S PHYSIOLOGICAL, BIOLOGICAL, OR BEHAVIORAL CHARACTERISTICS, OR AN INDIVIDUAL'S DEOXYRIBONUCLEIC ACID (DNA), THAT CAN BE USED, SINGLY OR IN COMBINATION WITH EACH OTHER OR WITH OTHER IDENTIFYING DATA, TO ESTABLISH INDIVIDUAL IDENTITY;

(IV) GEOLOCATION DATA;

(V) INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY INFORMATION, INCLUDING BROWSING HISTORY, SEARCH HISTORY, AND INFORMATION RELATED TO AN INDIVIDUAL'S INTERACTION WITH AN INTERNET WEBSITE, APPLICATION, OR ADVERTISEMENT;

(VI) INFORMATION FROM MULTIPLE SOURCES LISTED IN THIS PARAGRAPH THAT WHEN USED IN COMBINATION WITH EACH OTHER CAN BE USED TO ESTABLISH INDIVIDUAL IDENTITY; AND

(VII) 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.

(3) "PERSONALLY IDENTIFIABLE INFORMATION" DOES NOT INCLUDE:

(I) VOTER REGISTRATION INFORMATION;

(II) INFORMATION PUBLICLY DISCLOSED BY THE INDIVIDUAL WITHOUT DURESS OR COERCION; OR

(III) DATA RENDERED ANONYMOUS THROUGH THE USE OF TECHNIQUES INCLUDING OBFUSCATION, DELETION AND REDACTION, AND ENCRYPTION, SO THAT THE INDIVIDUAL IS NO LONGER IDENTIFIABLE.

(D) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS SECURITY PROTECTIONS THAT ALIGN WITH DEPARTMENT OF INFORMATION TECHNOLOGY POLICIES AND THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) OF 2014.

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

(F) "UNIT" MEANS AN EXECUTIVE AGENCY, A DEPARTMENT, A BOARD, A COMMISSION, AN AUTHORITY, OR A UNIT.

10–13A–02.

(A) (1) SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION, THIS SUBTITLE APPLIES ONLY TO THE COLLECTION, PROCESSING, AND SHARING OF PERSONALLY IDENTIFIABLE INFORMATION BY A UNIT.

(2) THIS SUBTITLE DOES NOT APPLY TO THE COLLECTION, PROCESSING, OR SHARING OF PERSONALLY IDENTIFIABLE INFORMATION EXCLUSIVELY FOR PURPOSES OF:

(I) PUBLIC HEALTH;

(II) PUBLIC SAFETY;

(III) STATE SECURITY; OR

(IV) THE INVESTIGATION AND PROSECUTION OF CRIMINAL OFFENSES.

(B) THIS SUBTITLE DOES NOT APPLY TO PERSONALLY IDENTIFIABLE INFORMATION THAT:

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

(2) AN INDIVIDUAL HAS CONSENTED TO HAVE PUBLICLY DISSEMINATED OR LISTED;

(3) EXCEPT FOR A MEDICAL RECORD THAT A PERSON IS PROHIBITED FROM REDISCLOSING UNDER § 4–302(D) OF THE HEALTH – GENERAL ARTICLE, IS DISCLOSED IN ACCORDANCE WITH THE FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT; OR

(4) IS DISCLOSED IN ACCORDANCE WITH THE FEDERAL FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT.

(C) (1) EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS SUBSECTION, THIS SUBTITLE APPLIES ONLY TO THE EXECUTIVE BRANCH OF STATE GOVERNMENT.

(2) THIS SUBTITLE DOES NOT APPLY TO A PUBLIC INSTITUTION OF HIGHER EDUCATION OR AN INSTRUMENTALITY OF THE STATE.

10–13A–03.

WHEN A UNIT IS DESTROYING RECORDS OF AN INDIVIDUAL THAT CONTAIN PERSONALLY IDENTIFIABLE INFORMATION OF THE INDIVIDUAL, THE UNIT SHALL TAKE REASONABLE STEPS TO PROTECT AGAINST UNAUTHORIZED ACCESS TO OR USE OF THE PERSONALLY IDENTIFIABLE INFORMATION, TAKING INTO ACCOUNT:

(1) THE SENSITIVITY OF THE RECORDS;

(2) THE NATURE OF THE UNIT AND ITS OPERATIONS;

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

(4) AVAILABLE TECHNOLOGY.

10–13A–04.

(A) (1) SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION, TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, OR DISCLOSURE, A UNIT THAT COLLECTS PERSONALLY IDENTIFIABLE INFORMATION OF AN INDIVIDUAL SHALL IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE NATURE OF THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTED AND THE NATURE OF THE UNIT AND ITS OPERATIONS.

(2) THE UNIT SHALL COMPLY WITH STANDARDS AND GUIDELINES, INCLUDING FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 199, FIPS 200, AND THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800 SERIES TO ENSURE THAT THE SECURITY OF ALL INFORMATION SYSTEMS AND APPLICATIONS ARE MANAGED THROUGH THE NIST RISK MANAGEMENT FRAMEWORK, WHICH REQUIRES THAT:

(I) THE SYSTEM IS CATEGORIZED BASED ON A FIPS 199 ANALYSIS;

(II) THE SECURITY CONTROLS ARE SELECTED BASED ON THE SECURITY CATEGORIZATION OF THE SYSTEM;

(III) THE CONTROLS ARE IMPLEMENTED WITHIN THE INFORMATION SYSTEM OR APPLICATION;

(IV) THE CONTROLS ARE ASSESSED BY A THIRD–PARTY ASSESSOR;

(V) THE SYSTEM IS AUTHORIZED TO OPERATE BY AN AUTHORIZING OFFICIAL OF THE UNIT WHO REVIEWS THE SECURITY AUTHORIZATION PACKAGE AND ACCEPTS THE RISKS IDENTIFIED;

(VI) THE IMPLEMENTED SECURITY CONTROLS ARE CONTINUOUSLY MONITORED FOR EFFECTIVENESS; AND

(VII) THE REASSESSMENT AND AUTHORIZATION OF SYSTEMS ARE COMPLETED ON AN ANNUAL BASIS.

(B) A UNIT THAT USES A NONAFFILIATED THIRD PARTY AS A SERVICE PROVIDER TO PERFORM SERVICES FOR THE UNIT AND DISCLOSES PERSONALLY IDENTIFIABLE INFORMATION ABOUT AN INDIVIDUAL UNDER A WRITTEN CONTRACT OR AGREEMENT WITH THE THIRD PARTY SHALL REQUIRE BY WRITTEN CONTRACT OR AGREEMENT THAT THE THIRD PARTY IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT:

(1) ARE APPROPRIATE TO THE NATURE OF THE PERSONALLY IDENTIFIABLE INFORMATION DISCLOSED TO THE NONAFFILIATED THIRD PARTY; AND

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

(C) (1) EACH UNIT SHALL UNDERTAKE ACTIVITIES COMPRISING THE COLLECTION, PROCESSING, AND SHARING OF PERSONALLY IDENTIFIABLE INFORMATION IN GOOD FAITH AND IN ACCORDANCE WITH THE REQUIREMENTS UNDER PARAGRAPH (2) OF THIS SUBSECTION.

(2) EACH UNIT SHALL:

(I) IDENTIFY AND DOCUMENT THE LEGAL AUTHORITY FOR ITS COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION;

(II) DESCRIBE THE PURPOSE OF THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTION AND PROVIDE NOTICE OF THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTION TO THE INDIVIDUAL AT THE TIME OF COLLECTION AND IN A PRIVACY NOTICE PROMINENTLY DISPLAYED ON THE UNIT'S WEB PRESENCE;

(III) ADOPT A PRIVACY GOVERNANCE AND RISK MANAGEMENT PROGRAM, AND IMPLEMENT REASONABLE SECURITY PROCEDURES AND PRACTICES, CONSISTENT WITH POLICIES AND STANDARDS ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY, IN ORDER TO ENSURE THAT CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ALL PERSONALLY IDENTIFIABLE INFORMATION IS MAINTAINED;

(IV) ESTABLISH PRIVACY REQUIREMENTS APPLICABLE TO CONTRACTORS, SERVICE PROVIDERS, AND OTHER THIRD PARTIES AND INCORPORATE THE REQUIREMENTS INTO AGREEMENTS ENTERED INTO WITH THE THIRD PARTIES;

(V) TAKE REASONABLE STEPS TO ENSURE THAT PERSONALLY IDENTIFIABLE INFORMATION COLLECTED IS ACCURATE, RELEVANT, TIMELY, AND COMPLETE;

(VI) TAKE REASONABLE STEPS TO IMPLEMENT MEANS TO MINIMIZE THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTED TO INFORMATION RELEVANT AND NECESSARY TO ADDRESS THE LEGALLY AUTHORIZED PURPOSE OF THE COLLECTION;

(VII) IMPLEMENT PROCESSES TO PROVIDE AN INDIVIDUAL ACCESS TO THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION AND TO ALLOW THE INDIVIDUAL TO CORRECT OR AMEND THE PERSONALLY IDENTIFIABLE INFORMATION PROCESSED BY THE UNIT; AND

(VIII) SUBJECT TO SUBSECTION (D) OF THIS SECTION, ESTABLISH CLEAR AND COMPREHENSIVE NOTICE PROVISIONS TO INFORM THE PUBLIC AND INDIVIDUALS OF UNIT PRACTICES AND ACTIVITIES REGARDING THE USE OF PERSONALLY IDENTIFIABLE INFORMATION.

(D) EACH UNIT SHALL:

(1) ADVISE AN INDIVIDUAL REQUESTED TO PROVIDE PERSONALLY IDENTIFIABLE INFORMATION WHETHER:

(I) THE PERSONALLY IDENTIFIABLE INFORMATION REQUESTED IS REQUIRED TO BE PROVIDED BY LAW; OR

(II) THE PROVISION OF THE PERSONALLY IDENTIFIABLE INFORMATION REQUESTED IS VOLUNTARY AND SUBJECT TO THE INDIVIDUAL'S

DISCRETION TO REFUSE TO PROVIDE THE PERSONALLY IDENTIFIABLE INFORMATION;

(2) PROVIDE AN INDIVIDUAL WITH CLEAR AND CONSPICUOUS MEANS TO ACCESS:

(I) THE TYPES OF PERSONALLY IDENTIFIABLE INFORMATION COLLECTED ABOUT THE INDIVIDUAL;

(II) THE TYPES OF SOURCES FROM WHICH THE PERSONALLY IDENTIFIABLE INFORMATION WAS COLLECTED;

(III) THE PURPOSE FOR COLLECTING THE PERSONALLY IDENTIFIABLE INFORMATION;

(IV) THE THIRD PARTIES WITH WHOM THE PERSONALLY IDENTIFIABLE INFORMATION IS SHARED; AND

(V) THE SPECIFIC PERSONALLY IDENTIFIABLE INFORMATION COLLECTED ABOUT THE INDIVIDUAL;

(3) INCLUDE THE MEANS PROVIDED UNDER ITEM (2) OF THIS SUBSECTION IN THE NOTICES PROVIDED TO THE INDIVIDUAL REGARDING THE COLLECTION, PROCESSING, AND SHARING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION;

(4) AT OR BEFORE THE POINT OF SHARING PERSONALLY IDENTIFIABLE INFORMATION, PROVIDE NOTICE TO AN INDIVIDUAL OF THE

UNIT'S SHARING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION, INCLUDING:

(I) THE NATURE AND SOURCES OF INFORMATION SHARED;

(II) THE PURPOSE FOR WHICH THE INFORMATION IS SHARED;

(III) THE RECIPIENTS OF THE SHARED INFORMATION;

(IV) THE AUTHORITY UNDER WHICH THE INFORMATION IS SHARED;

(V) ANY RIGHTS THE INDIVIDUAL HAS TO DECLINE THE UNIT'S SHARING OF PERSONALLY IDENTIFIABLE INFORMATION; AND

(VI) THE INDIVIDUAL'S RIGHT AND MEANS TO OBTAIN AND REVIEW THE PERSONALLY IDENTIFIABLE INFORMATION SHARED BY THE UNIT;

(5) PROVIDE AN INDIVIDUAL A PROCESS TO DELETE OR CORRECT PERSONALLY IDENTIFIABLE INFORMATION SHARED WITH THIRD PARTIES IF THE SHARING OF THE INFORMATION IS NOT REQUIRED BY LAW; AND

(6) PROVIDE AN INDIVIDUAL THE MEANS TO OPT OUT OF SHARING INFORMATION WITH THIRD PARTIES IF THE SHARING OF THE INFORMATION IS NOT REQUIRED BY LAW.

10-13A-05.

(A) (1) IN THIS SECTION, "BREACH OF THE SECURITY OF A SYSTEM" MEANS THE UNAUTHORIZED ACQUISITION OF COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF THE PERSONALLY IDENTIFIABLE INFORMATION MAINTAINED BY A UNIT.

(2) "BREACH OF THE SECURITY OF A SYSTEM" DOES NOT INCLUDE THE GOOD FAITH ACQUISITION OF PERSONALLY IDENTIFIABLE INFORMATION BY AN EMPLOYEE OR AGENT OF A UNIT FOR THE PURPOSES OF THE UNIT, PROVIDED THAT THE PERSONALLY IDENTIFIABLE INFORMATION IS NOT USED OR SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

(B) (1) IF A UNIT THAT COLLECTS COMPUTERIZED DATA THAT INCLUDES PERSONALLY IDENTIFIABLE INFORMATION OF AN INDIVIDUAL DISCOVERS OR IS NOTIFIED OF A BREACH OF THE SECURITY OF A SYSTEM, THE UNIT SHALL CONDUCT IN GOOD FAITH A REASONABLE AND PROMPT INVESTIGATION TO DETERMINE WHETHER THE UNAUTHORIZED ACQUISITION OF PERSONALLY IDENTIFIABLE INFORMATION OF THE INDIVIDUAL HAS RESULTED IN OR IS LIKELY TO RESULT IN THE MISUSE OF THE INFORMATION.

(2) (I) EXCEPT AS PROVIDED IN SUBPARAGRAPH (II) OF THIS PARAGRAPH, IF, AFTER THE INVESTIGATION IS CONCLUDED, THE UNIT DETERMINES THAT A MISUSE OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION HAS OCCURRED OR IS LIKELY TO OCCUR, THE UNIT OR THE NONAFFILIATED THIRD PARTY, IF AUTHORIZED UNDER A WRITTEN CONTRACT OR AGREEMENT WITH THE UNIT, SHALL NOTIFY THE INDIVIDUAL OF THE BREACH.

(II) UNLESS THE UNIT OR NONAFFILIATED THIRD PARTY KNOWS THAT THE ENCRYPTION KEY HAS BEEN BROKEN, A UNIT OR THE

NONAFFILIATED THIRD PARTY IS NOT REQUIRED TO NOTIFY AN INDIVIDUAL UNDER SUBPARAGRAPH (I) OF THIS PARAGRAPH IF:

1. THE PERSONALLY IDENTIFIABLE INFORMATION OF THE INDIVIDUAL WAS SECURED BY ENCRYPTION OR REDACTED; AND

2. THE ENCRYPTION KEY HAS NOT BEEN COMPROMISED OR DISCLOSED.

(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 UNIT DETERMINES THAT A MISUSE OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION HAS OCCURRED OR IS LIKELY TO OCCUR.

(4) IF, AFTER THE INVESTIGATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION IS CONCLUDED, THE UNIT DETERMINES THAT NOTIFICATION UNDER PARAGRAPH (2) OF THIS SUBSECTION IS NOT REQUIRED, THE UNIT SHALL MAINTAIN RECORDS THAT REFLECT ITS DETERMINATION FOR 3 YEARS AFTER THE DETERMINATION IS MADE.

(C) (1) A NONAFFILIATED THIRD PARTY THAT MAINTAINS COMPUTERIZED DATA THAT INCLUDES PERSONALLY IDENTIFIABLE INFORMATION PROVIDED BY A UNIT SHALL NOTIFY THE UNIT OF A BREACH OF THE SECURITY OF A SYSTEM IF THE UNAUTHORIZED ACQUISITION OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION HAS OCCURRED OR IS LIKELY TO OCCUR.

(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 NONAFFILIATED THIRD PARTY DISCOVERS OR IS NOTIFIED OF THE BREACH OF THE SECURITY OF A SYSTEM.

(3) A NONAFFILIATED THIRD PARTY THAT IS REQUIRED TO NOTIFY A UNIT OF A BREACH OF THE SECURITY OF A SYSTEM UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL SHARE WITH THE UNIT INFORMATION RELATING TO THE BREACH.

(D) (1) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OR (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 THE NOTIFICATION WILL NOT IMPEDE A CRIMINAL INVESTIGATION AND WILL NOT JEOPARDIZE HOMELAND OR NATIONAL SECURITY.

(E) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION MAY BE GIVEN:

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

(2) BY E–MAIL TO THE MOST RECENT E–MAIL ADDRESS OF THE INDIVIDUAL IN THE RECORDS OF THE UNIT IF:

(I) THE INDIVIDUAL HAS EXPRESSLY CONSENTED TO RECEIVE ELECTRONIC NOTICE; OR

(II) THE UNIT CONDUCTS ITS DUTIES PRIMARILY THROUGH INTERNET ACCOUNT TRANSACTIONS OR THE INTERNET;

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

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

(I) THE UNIT DEMONSTRATES THAT THE COST OF PROVIDING NOTICE WOULD EXCEED $100,000 OR THAT THE AFFECTED CLASS OF INDIVIDUALS TO BE NOTIFIED EXCEEDS 175,000; OR

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

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

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

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

(3) NOTIFICATION TO APPROPRIATE MEDIA.

(G) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION SHALL INCLUDE:

(1) TO THE EXTENT POSSIBLE, A DESCRIPTION OF THE CATEGORIES OF INFORMATION THAT WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED BY AN UNAUTHORIZED PERSON, INCLUDING WHICH OF THE ELEMENTS OF PERSONALLY IDENTIFIABLE INFORMATION WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED;

(2) CONTACT INFORMATION FOR THE UNIT MAKING THE NOTIFICATION, INCLUDING THE UNIT'S ADDRESS, TELEPHONE NUMBER, AND TOLL–FREE TELEPHONE NUMBER IF ONE IS MAINTAINED;

(3) THE TOLL–FREE TELEPHONE NUMBERS AND ADDRESSES FOR THE MAJOR CONSUMER REPORTING AGENCIES; AND

(4) (I) THE TOLL–FREE TELEPHONE NUMBERS, ADDRESSES, AND WEBSITE ADDRESSES FOR:

1. THE FEDERAL TRADE COMMISSION; AND

2. THE OFFICE OF THE ATTORNEY GENERAL; AND

(II) A STATEMENT THAT AN INDIVIDUAL CAN OBTAIN INFORMATION FROM THESE SOURCES ABOUT STEPS THE INDIVIDUAL CAN TAKE TO AVOID IDENTITY THEFT.

(H) (1) BEFORE GIVING THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION, A UNIT SHALL PROVIDE NOTICE OF A BREACH OF THE SECURITY OF A SYSTEM TO THE OFFICE OF THE ATTORNEY GENERAL.

(2) IN ADDITION TO THE NOTICE REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION, A UNIT SHALL PROVIDE NOTICE OF A BREACH OF SECURITY TO THE DEPARTMENT OF INFORMATION TECHNOLOGY.

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

(J) COMPLIANCE WITH THIS SECTION DOES NOT RELIEVE A UNIT FROM A DUTY TO COMPLY WITH ANY OTHER REQUIREMENTS OF FEDERAL LAW RELATING TO THE PROTECTION AND PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION.

10-13A-06.

(A) IF A UNIT IS REQUIRED UNDER § 10-13A-05 OF THIS SUBTITLE TO GIVE NOTICE OF A BREACH OF THE SECURITY OF A SYSTEM TO 1,000 OR MORE INDIVIDUALS, THE UNIT 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 PERSONALLY IDENTIFIABLE INFORMATION OF RECIPIENTS OF NOTICES OF THE BREACH OF THE SECURITY OF A SYSTEM.

10-13A-07.

A UNIT OR NONAFFILIATED THIRD PARTY THAT COMPLIES WITH § 501(B) OF THE FEDERAL GRAMM–LEACH–BLILEY ACT; 15 U.S.C. § 6801, § 216 OF THE FEDERAL FAIR AND ACCURATE CREDIT TRANSACTIONS ACT; 15 U.S.C. § 1681W DISPOSAL OF RECORDS; 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 OF THOSE ENACTMENTS, SHALL BE DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.".

On pages 6 through 19, strike in their entirety the lines beginning with line 4 on page 6 through line 13 on page 19, inclusive.

On page 19, in line 14, strike "6." and substitute "2."; in lines 14 and 15, strike ", except as provided in Sections 4 and 5 of this Act,"; and in line 15, strike "October 1, 2019" and substitute "July 1, 2021".