GENERAL COMMITTEE MEETING

Thursday, January 16, 2020
3:00 PM to 4:00 PM

Healthcare Leadership Council
750 9th Street, NW, Suite 500 Washington, D.C. 20001
Conference Line: 857-232-0157, **Code:** 30-40-73

1. **Welcome and Introductions**

2. **Legislative Update**
   a. House Energy and Commerce — Attachment 1
   b. Senate Commerce
      i. Wicker — Attachment 2
      ii. Cantwell — Attachment 3

3. **Telephone Consumer Protection Act (TCPA)**

4. **OMB Meeting Debrief**

5. **Privacy Round Up December 2019** — Attachment 4

6. **FDA Data Infrastructure Meeting/Request for Comment** — Attachment 5

[DISCUSSION DRAFT]
DATE

116TH CONGRESS
1ST SESSION

H. R. __

To **[___]**, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES
_____ introduced the following bill; which was referred to the Committee on _____

A BILL

To **[___]**, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "_____ Act of 2019".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. SENSE OF CONGRESS; PRIVACY BILL OF RIGHTS.

It is the sense of Congress that— [TBD]

SEC. 3. TRANSPARENCY.

(a) REGULATIONS REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that are limited to the provisions included in this section. Such regulations shall require the following:

(1) REQUIRED PRIVACY POLICY.—A covered entity shall develop and make publicly available at all times and in a machine-readable format, a privacy policy, in a manner that is clear, easily understood, and written in plain and concise language, that includes—

(A) the categories of covered information that the covered entity processes;

(B) how and under what circumstances covered information is collected directly from the individual;

(C) the categories and the sources of any covered information processed by a covered entity that is not collected directly from the individual;

(D) a description of all of the purposes for which the covered entity processes covered information, including—

(i) for any sensitive information, a detailed description of all of the purposes for which the covered entity processes such information stated with particularity and whether the covered entity shares such sensitive information with any third party;

(ii) a description of whether and how the covered entity customizes products or services, or adjusts the prices of products or services for individuals based in any part on processing of covered information;

(iii) a description of whether and how the covered entity, the covered entity's processors, and third parties with whom the covered entity discloses covered information, deidentifies information, including the methods used to deidentify such information;

(iv) a description of whether and how the covered entity, the covered entity's processors, and third parties with whom the covered entity discloses covered information, generates or uses any **[**consumer score**]** to make decisions

concerning an individual, and the source or sources of any such **[**consumer score**]**;

(E) a description of how long and the circumstances under which the covered entity retains covered information;

(F) a description of all of the purposes for which the covered entity discloses covered information with processors, and, on a biennial basis, the categories of such processors;

(G) a description of whether and for what purposes the covered entity discloses information to third parties, and, on a biennial basis, the categories of such third parties;

(H) whether a covered entity sells or otherwise shares covered information with data brokers or processes covered information for targeted advertising;

(I) whether a covered entity collects covered information about individuals over time and across different websites or mobile applications when an individual uses the covered entity's website or mobile application;

(J) how individuals can exercise their rights to access, correct, and delete such individual's covered information as required under Section 5;

(K) how individuals can exercise their rights under Sections 6, 7, and 8, including how to modify and withdraw consent for the processing of covered information, and the consequences of exercising those rights;

(L) the effective date of the notice; and

(M) how the covered entity will communicate material changes of the privacy policy to individuals.

(2) ANNUAL FILINGS TO THE FTC.—Each covered entity that either has annual revenue in excess of **[**$250,000,000**]** in the prior year or that processes covered information of more than **[**10,000,000**]** individuals **[**or consumer devices**]** in the prior year, shall be required to submit to the Commission, on an annual basis, a privacy filing that includes:

(A) a detailed and granular description of each of the requirements in subsection (a)(1);

(B) a detailed and granular description of—

(i) the ways in which each category of covered information is processed by the covered entity; and

(ii) how long the covered entity keeps, stores, or retains covered information for each identified purpose (C) an assessment of the risks posed to individuals as a result of the covered entity's processing of covered information, and a general description of the measures the covered entity has taken or will take to address such risks;

(D) the name and contact information of the privacy protection officer required under Section 4(c);

(E) a description of any material changes in the covered entity's privacy policies or practices since the covered entity's most recent prior disclosure to the Commission; and

(F) a description of any security incidents that required the covered entity to provide notice of the security incident under any federal or State law to individuals, a consumer reporting agency, or to a State attorney general or other State or federal government entity, and the results of all audits or investigations undertaken following any such security incidents.

(3) OFFICER CERTIFICATION.—For each covered entity that submits an annual filing under paragraph (2), the covered entity's **[**principal executive officer**]** and the privacy protection officer required under Section 4(c) of this Act, shall be required to certify in each annual filing submitted under this Act that—

(A) the signing officer has reviewed the filing;

(B) based on such officer's knowledge, the filing does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements, in light of the circumstances under which such statements were made, not misleading;

(C) based on such officer's knowledge, the filing fairly presents in all material respects the privacy practices of the covered entity;

(D) the signing officer—

(i) is responsible for establishing and maintaining safeguards and controls to protect the privacy of and ensure the lawful processing of covered information;

(ii) has evaluated the effectiveness of such safeguards and controls as part of the assessment required under paragraph (3)(B); and

(iii) has provided all material conclusions about the effectiveness of such safeguards and controls.

[(4) RULE OF CONSTRUCTION.—The principal executive officer may rely on information provided by the privacy protection officer, independent audits, or other sources provided that the principle executive officer has conducted a reasonable review of the information provided and acted in good faith.**]**

(5) The filings required by paragraph (a)(2) may supplement the information provided to individuals under paragraph (a)(1) but shall not be sufficient to satisfy that paragraph.

(6) The Commission shall make publicly available on the website of the Commission the disclosures required under paragraph (a)(2). The Commission may withhold information required under such paragraph if the Commission determines such information should not be public. If the Commission withholds any information, the Commission shall make publicly available on the website the category of information withheld and the reasons for withholding it.

(b) ASSESSMENT AND COLLECTION OF FILING FEES.—

(1) The Commission shall assess and collect filing fees established in paragraph (2), which shall be paid by covered entities who are required to submit annual filings required by subsection (a)(2) and the regulations promulgated under this Section. For purposes of this Act, no annual filing shall be considered submitted until payment of the fee required by this subsection. Fees collected pursuant to this section shall be used to carry out the authorities of the Commission under this Act and shall remain available until expended.

(2) The filing fee referred to in subsection (a) shall be **[**$15,000**]**, subject to paragraph (3).

(3) Not later than January 15 of each year after the date of enactment of this Act, the Commission may adjust the filing fee provided in paragraph (2) to account for the percentage by which the Consumer Price Index for the month of October preceding the date of the adjustment exceeds the Consumer Price Index for the month of October in the preceding year.

(c) STANDARD SHORT-FORM STATEMENTS AND GRAPHIC ICONS FOR PRIVACY PRACTICES—

(1) Not later than **[**180 days**]** after the date of the enactment of this Act, the Commission shall conduct a study to determine the most effective method of communicating common privacy practices in short-form privacy statements, graphic icons, or other means determined by the Commission that disclose how a covered entity collects covered information, the purposes for which the covered entity collects such information, and, if applicable, the category of third parties the covered entity shares such information with. The Commission shall submit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science,

and Transportation of the Senate with the results of the study. The report shall also be made publicly available on the website of the Commission.

(2) After completion of the study and not later than **[**1 year**]** after the date of the enactment of this Act, the Commission shall finalize regulations based on the results of such study that require covered entities to communicate the covered entity's privacy practices for the information described in paragraphs 1(A)-(B), 1(C)(i)-(iii), 1(E) and 1(F) of subsection (a), and any other information as the Commission may determine.

(3) The method of communicating common privacy practices required under this section shall be clearly and conspicuously provided to consumers at the location and time at which covered information is first collected by a covered entity in the form and manner determined by the Commission in the rulemaking required under this section.

SEC. 4. PRIVACY PROGRAM.

(a) Not later than **[**1 year**]** after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that are limited to the provisions included in this section. Such regulations shall require each covered entity to establish and implement reasonable policies, practices, and procedures regarding the processing of covered information—

(1) designed to—

(A) comply with applicable privacy laws;

(B) consider the mitigation of privacy risks throughout every stage of the covered entity's products and services, including their design, development, launch, and implementation; and

(C) implement reasonable training and safeguards within the covered entity to promote compliance with all privacy laws applicable to covered information the covered entity processes and mitigate privacy risks;

(2) taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by such covered entity;

(B) the sensitivity of the covered information processed by the covered entity;

(C) the volume of covered information processed by the covered entity;

(D) the number of individuals **[**or consumer devices**]** to which the covered information processed by the covered entity relates; and

(E) the cost of implementing the program.

(b) ADDITIONAL REQUIREMENTS—The regulations required pursuant to paragraph (a) shall require a covered entity to:

(1) designate—

(A) for covered entities with annual revenue in excess of **[**$25,000,000**]** in the prior year, a privacy protection officer as required under subsection (c); or

(B) for all other covered entities, an owner or an officer or employee who reports directly to the owner or highest official within the covered entity to oversee the privacy program;

(2) establish processes to monitor, manage and enforce the covered entity's privacy practices, and demonstrate the covered entity's compliance with law;

(3) identify the purposes for which the covered entity processes covered information;

(4) establish processes to assess the risks to individuals resulting from the covered entity's processing of covered information in a manner prohibited by this Act before engaging in any such processing, including through the introduction of new products or services;

(5) establish a process to periodically review and update the covered entity's privacy policies, practices, and procedures as necessary;

(6) establish and implement controls to monitor and mitigate known or reasonably foreseeable risks resulting from the covered entity's processing of covered information; and

(7) establish processes for privacy training and education at the covered entity.

(c) PRIVACY PROTECTION OFFICERS.—A covered entity with annual revenue in excess of **[**$25,000,000**]** the prior year shall designate at least one appropriately qualified employee who reports directly to the highest official at the covered entity as a privacy protection officer who shall, either directly or through a supervised designee —

(1) educate and train employees about compliance requirements;

(2) train employees involved in processing of covered information;

(3) conduct regular, comprehensive audits to ensure compliance and make records of such audits available to enforcement authorities upon request;

(4) maintain updated, clear, and understandable records of all data security practices undertaken by the covered entity; and

(5) serve as the point of contact between the covered entity and enforcement authorities.

SEC. 5. RIGHT TO ACCESS AND DELETE COVERED INFORMATION AND REQUEST CORRECTIONS OF INACCURATE INFORMATION.

(a) REGULATIONS.—Not later than **[**1 year**]** after the date of enactment of this Act, the Commission shall finalize regulations under section 553 of title 5, United States Code, that are limited to the provisions included in this section. Such regulations shall require the following:

(1) CONFIRMATION OF PROCESSING.—Upon the request of an individual, a covered entity shall be required to provide confirmation to an individual as to whether the covered entity processes covered information pertaining to the individual.

(2) RIGHT OF ACCESS—Subject to the exemptions in paragraph (b), if a covered entity processes covered information pertaining to an individual, the covered entity shall be required, upon the request of the individual, to provide the individual with access to such covered information, including any consumer profile or **[**consumer score**]** of the individual, and provide a description of—

(A) the categories of covered information processed about the individual;

(B) the purposes for which the covered entity processes each category of covered information about the individual;

(C) the processors and third parties to which the covered entity has disclosed or will disclose the covered information;

(D) the sources from which covered information was collected other than the individual;

(E) if possible, how long the covered information will be kept, retained or stored, or, if not possible, the criteria used for determining how long the covered information will be retained or stored; and

(F) for any **[**consumer score**]** relating to the individual, a description of how such **[**consumer score**]** is used to make decisions concerning the individual and the source of such **[**consumer score**]** if not created by the covered entity.

(3) RIGHT TO CORRECT.—Subject to the exemptions in paragraph (b), if a covered entity processes covered information pertaining to an individual, the covered entity shall be required to provide the individual a means to dispute the accuracy or completeness of such covered information and correct inaccurate information. If the

covered entity cannot correct such information, the covered entity shall disclose to such individual why it cannot.

(4) SPECIAL REQUIREMENTS FOR CERTAIN COVERED ENTITIES.—

(A) PUBLIC RECORD INFORMATION HELD BY CERTAIN COVERED ENTITIES.—Each information broker and each covered entity that either has annual revenue in excess of **[**$250,000,000**]** in the prior year or that processes covered information of more than **[**10,000,000**]** individuals **[**or consumer devices**]** in the prior year, upon receipt of a request from an individual to dispute the accuracy or completeness of covered information under paragraph (3), shall be required to, if the covered information is public record information—

(i) inform the individual of the source of the information and where a request for correction may be directed, if such information is reasonably available; and

(ii) if the individual provides proof that the public record has been corrected or that the information broker or covered entity was reporting the information incorrectly, correct the inaccuracy in the records of the information broker or covered entity.

(B) ALTERNATIVE OPTION FOR SMALL BUSINESSES.—A small business that maintains covered information may, in lieu of complying with the correction requirements of this section, delete such covered information of the individual in its entirety, subject to subsection (b).

(5) RIGHT TO DELETE.—Subject to the exemptions in paragraph (b), if a covered entity processes covered information pertaining to an individual, the covered entity shall be required to delete upon the request of the individual the covered information, including any particular item of covered information, retained or stored by the covered entity pertaining to the individual.

(b) EXCEPTIONS.—The regulations required under subsection (a) shall include exceptions to the rights of access, correction, or deletion as follows:

(1) A covered entity shall not be required to provide access to or to correct or delete an individual's covered information under subsection (a) if—

(A) the covered entity cannot reasonably verify the individual's identity;

(B) the covered entity is limited from doing so by law, legally recognized privilege, or other legal obligation; or

(C) the covered entity makes an individualized determination that fulfilling the request would create a legitimate risk to the privacy, security, or safety of someone other than the individual or to the covered entity.

(2) A covered entity shall not be required to correct or delete an individual's covered information under subsection (a) if—

(A) retention of the information is necessary to:

(i) complete the transaction for which the covered information was collected;

(ii) provide a product or service affirmatively requested by the individual or to effectuate product recalls;

(iii) perform a contract with the individual, including billing, financial reporting, and accounting;

(iv) detect or prevent security incidents;

(v) protect or defend against fraudulent or illegal activity, or prosecute persons responsible for such activity; or

(vi) debug or identify and repair errors that impair existing functionality;

(B) the covered information is used in public or peer-reviewed scientific, medical, or statistical research in the public interest that adheres to commonly accepted ethical standards or laws, with informed consent consistent with 21 CFR 50.20, provided that the research must already be in progress at the time of an individual's request to delete the covered information; or

[(C) subject to paragraph (4) of subsection (a), the covered information is publicly available information**]**.

(3) The Commission may consider and establish by regulation additional limited exceptions consistent with the intent of this section.

(c) OBLIGATIONS OF COVERED ENTITIES TO PROVIDE MECHANISMS FOR THE EXERCISE OF INDIVIDUAL RIGHTS AND CONSUMER REDRESS—

(1) In promulgating regulations under subsection (a), the Commission shall require covered entities to provide mechanisms for the exercise of individual rights and options for consumer redress as follows:

(A) MECHANISMS TO EXERCISE RIGHTS—A covered entity shall provide a mechanism for individuals to exercise the rights provided under this section in a form that is clear and conspicuous, easy-to-use, and made available—

(i) without requiring the individual to establish an account with the covered entity; and

(ii) in a language other than English if the covered entity transacts business with individuals in another language.

(B) REASONABLE VERIFICATION OF INDIVIDUALS.—The regulations required under subsection (a) shall include—

(i) requirements that covered entities establish reasonable procedures to verify the identity of individuals who exercise the rights provided under subsection (a);

(ii) standards for the reasonableness of verification of individuals, considering the sensitivity of the covered information processed or retained by the covered entity and the purposes for which such covered information is processed; and

(iii) a requirement that information collected from an individual to verify the identity of the individual that the covered entity did not have before such collection cannot be used for any other purpose.

(C) RESPONSES TO REQUESTS TO EXERCISE RIGHTS—A covered entity shall comply with an individual's request to exercise a right provided under subsection (a) within 45 days of receiving a verifiable request from the individual. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the individual is provided notice of the extension within the first 45-day period.

(i) A covered entity shall comply with an individual's request under subsection (a), even if the request is received from another covered entity, if the receiving covered entity can verify that the request is originally from the individual.

(ii) If a covered entity denies an individual's request to exercise an individual right under this section, the covered entity shall inform the individual no later than 45 days after receiving the request and shall—

(I) inform the individual of the reasons for denying the request; and

(II) provide contact information for the Commission and for the individual's State attorney general.

(iii) A covered entity must establish a reasonable means by which an individual can appeal a denial of a request within 45 days.

(iv) A covered entity shall not unreasonably fail to comply with an individual's request to exercise an individual right under this section.

(d) PROHIBITION ON FEES—A covered entity shall be prohibited from charging a fee to an individual for exercising a right under subsection (a) of this section, except that a covered entity may charge a reasonable fee to recover the cost of a request for access to covered information if an individual seeks access to such information more than twice in a 12-month period.

(e) RULE OF CONSTRUCTION—Nothing in this section shall be interpreted to require a covered entity to take any action that would convert information that is not covered information into covered information.

SEC. 6. LIMITATIONS ON PROCESSING OF COVERED INFORMATION.

[(a) IN GENERAL.—

(1) Not later than **[**1 year**]** after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that are limited to the provisions included in this section.**]**

(2) GENERAL PROHIBITION—A covered entity may not process the covered information of an individual without consent.

(b) PROCESSING THAT DOES NOT REQUIRE AFFIRMATIVE CONSENT.—

(1) IN GENERAL.—Consent for the processing of covered information is implied to the extent the processing is consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual, subject to the restrictions in subsection (d)(2).

(2) CONSISTENT WITH THE CONTEXT OF THE INTERACTION—Processing shall be deemed to be consistent with the context of the interaction between an individual and a covered entity if such processing is—

(A) expected in light of the nature of the individual's transaction or with the individual's existing relationship with the covered entity;

(B) for purposes of—

(i) order fulfillment;

(ii) providing a product or service specifically requested by the individual;

(iii) billing and auditing related to the interaction, including customer warranty;

or

(iv) internal data analytics for the purposes of **[**product development and improvement**]**;

(C) necessary for compliance with a legal obligation or specifically authorized by law;

(D) necessary to—

(i) verify identity and the detection and prevention of fraudulent, malicious, or illegal activity, or prosecute persons responsible for such activity;

(ii) defend against actual or potential security threats;

(iii) prevent imminent danger to the personal safety of an individual or group of individuals;

(iv) network management and security, including debugging to identify and repair errors that impair existing functionality; or

(E) for purposes of first-party marketing, subject to the limitations provided in subparagraph (c); or

[(F) of publicly available information**]**.

(F) RULEMAKING.—The Commission may promulgate regulations under section 553 of title 5, United States Code, for additional processing that may not require consent consistent with the intent of this section.

(3) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance to provide more clarity regarding what constitutes reasonable consumer expectations with respect to individual's interactions with covered entities.

[(c) OPT-OUT REQUIRED FOR PROCESSING OF COVERED INFORMATION FOR FIRST-PARTY MARKETING PURPOSES.—

(1) IN GENERAL—A covered entity that processes an individual's covered information for purposes of first-party marketing under subparagraph (b)(2)(E) **[**must have an existing relationship with the individual**]** and such covered entity shall provide the individual with the ability to opt out of such processing.

(2) TRACKING EXCLUDED—A covered entity that has a first-party relationship with an individual for purposes of providing a specific product or service **[**shall not engage in tracking an individual's activities across third-party websites, applications, or other online products or services, unless such covered entity obtains express, affirmative consent in the form and manner provided in subsection (d).**]**

(3) REQUIREMENTS FOR OPT-OUT.—A covered entity shall provide a reasonable and easy means for an individual to exercise the opt-out required under subparagraph (c)(1) presented in easily understandable, concise, accurate, and clear language.

(d) EXPRESS, AFFIRMATIVE CONSENT REQUIRED FOR MOST OTHER PROCESSING OF COVERED INFORMATION.—

(1) A covered entity shall provide a clear and concise notice and obtain express, affirmative consent of the individual, in the form and manner provided in subsection (e), before processing covered information for a purpose that is not consistent with reasonable consumer expectations within the context of the interaction between the covered entity and an individual.

(2) Such notice and consent are also required before—

(A) processing sensitive information;

[(C) processing covered information for public and peer reviewed scientific, medical, or statistical research in the public interest, provided that such research adheres to commonly accepted ethical standards and all applicable laws, and with informed consent consistent with 21 CFR 50.20;**]**

[(D) any use of covered information for a purpose different from the purposes for which such covered information was collected;**]**

(E) any material changes to the processing of covered information.; or

[(F) other processing of covered information as determined by the Commission through the promulgation of regulations under section 553 of title 5, United States Code.**]**

(e) CONDITIONS FOR EXPRESS, AFFIRMATIVE CONSENT.—

[(1) REGULATIONS—The Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each covered entity that

processes covered information under subsection (c) to obtain the individual's express, affirmative consent—**]**

(A) in a manner that is freely given, specific, informed, and unambiguous;

(B) separately, for each use of specific types of covered information at the time such covered information is to be processed;

(D) through the primary medium used to offer or deliver the covered entity's product or service; and

(E) presented, before such processing occurs, at a time and in a context in which the individual would reasonably expect to make choices concerning such processing.

[(2) WITHDRAWAL OF CONSENT—The Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each covered entity to provide an individual a reasonable and easy mechanism to withdraw his or her consent at any time in a manner that is as easy as the mechanism to give consent.**]**

(3) RULE OF CONSTRUCTION—The withdrawal of consent shall not be construed to affect the lawfulness of any processing based on consent before its withdrawal.

(f) PROHIBITED INFORMATION PROCESSING PRACTICES.—

(1) PROHIBITION ON PRETEXTING.—

(A) PROHIBITION ON OBTAINING COVERED INFORMATION BY FALSE PRETENSES.—It shall be unlawful for a covered entity to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed, to any other person any covered information by—

(i) making a false, fictitious, or fraudulent statement or representation to any person; or

(ii) providing any document or other information to any person that the covered entity has actual knowledge that it is forged, counterfeit, lost, stolen, or fraudulently obtained, or to contain a false, fictitious, or fraudulent statement or representation.

(B) PROHIBITION ON SOLICITATION TO OBTAIN COVERED INFORMATION UNDER FALSE PRETENSES.—It shall be unlawful for a covered entity to request a person to obtain covered information relating to any other person, if the covered entity had actual knowledge that the person to whom such a request is made will obtain or attempt to obtain such information in the manner described in subparagraph (A).

(i) PROHIBITED PRACTICES.—Except to the extent that processing is necessary to provide or add to the functionality of a product, service, or specific feature that an individual has requested or is consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual, and subject to the exceptions provided in paragraph (3) and the regulations promulgated pursuant to paragraph (4), a covered entity may not process—

(A) biometric information for purposes of identifying an individual or to verify an individual's identity;

(B) precise geolocation information linkable to an identifiable individual or **[**consumer device;**]**

(C) covered information to attribute a **[**consumer device or devices**]** to a specific individual using probabilistic methods, such as algorithms or usage patterns;

(D) covered information obtained through a microphone or camera of a consumer device;

(E) the contents of an individual's communications or the parties to such communications; or

(F) health information.

(3) EXCEPTIONS.—Nothing in this section shall prohibit a covered entity from engaging in the practices described in paragraph (2) if necessary solely for purposes of—

(A) detecting and preventing security incidents;

(B) protecting and defending against fraudulent or illegal activity;

(C) preventing imminent danger to the personal safety of an individual or group of individuals;

(D) debugging or repairing errors that impair existing functionality;

(E) complying with any Federal, State, or local law, rule, regulation, or other legal obligation, including civil, criminal, or regulatory inquiries, investigations, subpoenas, disclosures of information required by a court order or other properly executed compulsory process;

(F) Investigate, exercise, or defend legal claims arising out of the processing of covered information that is the subject of such claim;

(G) Protect the legal rights of the individual or of another individual;

(4) EXEMPTIONS.—The Commission shall promulgate regulations under section 553 of title 5, United States Code, to allow covered entities to petition the Commission for an exemption to particular practices prohibited in paragraph (2).

[(5) NO CONSENT FOR PROHIBITED PRACTICES.—It shall be unlawful for a covered entity to seek to obtain consent from an individual to engage in any of the practices described in paragraph (2).**]**

SEC. 7. DATA RETENTION.

(a) Not later than **[**1 year**]** after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that are limited to the provisions included in this section. Such regulations shall require the following:

(1) RETENTION LIMITATIONS.—Subject to the exceptions provided in paragraph (2), a covered entity shall not keep, retain, or otherwise store covered information for longer than is reasonably necessary for the purposes for which the covered information is processed.

(2) EXCEPTIONS.—Further retention of covered information shall not be deemed incompatible with the initial purposes of processing if such processing is necessary and done solely for the purposes of:

(A) compliance with laws, regulations, or other legal obligations;

(B) detecting and preventing security threats, fraud, theft, unauthorized transactions, or illegal activities; or

(C) preventing risks to the health or safety of an individual or group of individuals;

(D) debugging or repairing errors that impair existing functionality; or

(E) any other exception determined by the Commission to promote the public interest and protect the privacy of individuals in the rulemaking authorized in this section.

SEC. 8. LIMITATION ON DISCLOSING COVERED INFORMATION TO PROCESSORS AND THIRD PARTIES.

(a) REGULATIONS REQUIRED.—Not later than **[**1 year**]** after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that are limited to the provisions included in this section. Such regulations shall require the following:

(1) A covered entity shall not disclose covered information to a processor—

(A) unless the covered entity has a written agreement with such processor that—

(i) prohibits the processing of covered information for any purpose other than the purposes for which the covered entity disclosed the covered information to the processor;

[(ii) prohibits the processing of covered information for any purpose for which the covered entity does not have consent;**]**

(iii) requires the processor **[**provide at least the same privacy and security protections as the covered entity / comply with this Act**]**;

(iv) requires the processor to comply with any request by the covered entity in response to an individual's request to access, correct, or delete pursuant to Section 5 of this Act;

(v) requires the processor to comply with any request by the covered entity for the covered entity to fulfill Section 7 of this Act;

(vi) prohibits the processor from engaging another processor without a written agreement from the covered entity and a written agreement with the other processor that the other processor shall submit to the same obligations imposed on the processor;

(vii) requires the processor to make available to the covered entity all information necessary to demonstrate the covered entity's compliance with this Act; and

(viii) requires the processor to allow for and contribute to audits, including inspections, conducted by the covered entity or another auditor mandated by the covered entity; or

(B) for any purpose that is inconsistent with reasonable consumer expectations within the context of the individual's interaction with the covered entity or for any prohibited purpose, as provided in Section 6.

(2) A covered entity shall not disclose covered information to a third party unless the covered entity obtains prior express, affirmative consent of the individual to whom the covered information pertains, as provided under Sec. 6(d) of this Act, and obtains a written agreement with the third party that—

(A) specifies all of the purposes for which the third party may process the covered information;

(B) prohibits the third party from further processing such covered information for any purpose other than what is necessary for the purposes described in subparagraph (A);

(C) prohibits such third party from processing covered information in any manner that is—

(i) inconsistent with the consent of the individual to whom the covered information pertains, as provided under Section 6; or

(ii) for any prohibited purpose as provided under Section 6(e); and

(D) such third party shall **[**provide at least the same privacy and security protections as the covered entity / comply with this Act**]**.

(3) A covered entity shall not sell, license, or lease sensitive information to a third party unless the individual provided express, affirmative consent prior to the selling, licensing, or leasing of such sensitive information and such third party is a covered entity that must comply with this Act.

(4) A covered entity shall be required to perform reasonable due diligence in selecting processors and third parties and shall exercise reasonable oversight over all such processors and third parties, to assure compliance with all of the requirements of this Act.

(5) A covered entity that has actual knowledge that a processor or third party has violated this Act, or any regulation of the Commission promulgated under this Act, shall, to the extent practicable, promptly take steps to ensure compliance with the Act and promptly report to the Commission that such a violation occurred.

(b) EXCEPTIONS.—Nothing in this section shall prohibit a covered entity from disclosing covered information to a processor or third party—

(1) solely for the purposes of any exception provided in Section 6(f)(3);

[(2) if such covered information is publicly available information; or

(3) if the covered information is pseudonymized information and the third-party recipient cannot, or by written contract will not, link such information to specific individuals and cannot share such pseudonymized information with any other party**]**.

SEC. 9. DATA SECURITY.

(a) GENERAL SECURITY POLICIES, PRACTICES, AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that are limited to the provisions included in this section. Such regulations shall require each covered entity and processor to implement and maintain reasonable administrative, technical, and physical security measures, policies, practices, and procedures to protect and secure covered information against unauthorized access and acquisition taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by such covered entity;

(B) the sensitivity of any covered information at issue;

(C) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(D) the cost of implementing such safeguards.

(2) REQUIREMENTS.—Such regulations shall require the policies, practices, and procedures to include the following:

(A) a written security policy with respect to the collection, use, sale, other dissemination, and maintenance of such covered information.

(B) the identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(C) a process for identifying and assessing any reasonably foreseeable vulnerabilities in the system or systems maintained by such covered entity that contains such covered information, which shall include regular monitoring for a breach of security of such system or systems.

(D) a process for taking preventive and corrective action to mitigate against any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software, and for regular testing or otherwise monitoring the effectiveness of the safeguards.

(E) A process for determining if data is no longer needed and disposing of data containing covered information by shredding, permanently erasing, or otherwise modifying the covered information contained in such data to make such covered information permanently unreadable or indecipherable.

(F) A process for overseeing persons who have access to covered information, including through Internet-connected devices, by—

(i) taking reasonable steps to select and retain persons that are capable of maintaining appropriate safeguards for the covered information or Internet-connected devices at issue; and

(ii) requiring all such persons to implement and maintain such security measures.

(G) A process for employee training and supervision for implementation of the policies, practices, and procedures required by this subsection.

(H) A written plan or protocol for internal and public response in the event of a breach of security.

(3) PERIODIC ASSESSMENT AND CONSUMER PRIVACY AND DATA SECURITY MODERNIZATION.—Not less frequently than every 12 months, each covered entity shall monitor, evaluate, and adjust, as appropriate, the data security program of such covered entity in light of any relevant changes in—

(A) technology;

(B) internal or external threats and vulnerabilities to covered information; and

(C) the changing business arrangements of the covered entity, such as—

(i) mergers and acquisitions;

(ii) alliances and joint ventures;

(iii) outsourcing arrangements;

(iv) bankruptcy; and

(v) changes to personal information systems.

(4) SUBMISSION OF POLICIES TO THE FTC.—The regulations promulgated under this subsection shall require each covered entity to notify the Commission of a breach of security and to submit its security policies to the Commission upon such notification. Such information shall be considered privileged and confidential for the purposes of section 552(b)(4) of title 5, United States Code.

SEC. 10. SPECIAL REQUIREMENTS ON INFORMATION BROKERS.

(a) NOTICE ON WEBSITE OF INFORMATION BROKER.—An information broker shall place a clear and conspicuous notice on the Internet website of the information broker (if the information broker maintains such a website) notifying consumers that the entity is an

information broker using specific language that the Commission shall determine through rulemaking and providing a link to the website established under subsection (c).

(b) REQUIRED AUDIT LOG OF ACCESSED AND TRANSMITTED INFORMATION.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations to require an information broker to establish measures that facilitate the auditing of any internal or external access to, or disclosure of, any covered information relating to an individual processed by such information broker.

(c) FTC REGISTRY OF INFORMATION BROKERS.—

(1) Not later than **[**1 year**]** after the date of enactment of this Act, the Commission shall promulgate regulations that are limited to the provisions included in this section. Such regulations shall to require each information broker that processes covered information **[**of more than 5,000 individuals per year**]** to register with the Commission and provide—

(A) a legal name of the information broker and any other related entities through which the information broker processes covered information;

(B) a description of the categories of information the information broker processes;

(C) a description of any **[**consumer score**]** the information broker sells, licenses, or otherwise discloses to third parties;

(D) the contact information of the information broker, including a telephone number, an e-mail address, a website, and a physical mailing address; and

(E) a link to a website through which an individual may easily exercise the rights provided under subsection (b) of this Section.

(2) The Commission shall establish and maintain on an Internet website a searchable, central registry of information brokers that—

(A) is accessible to the general public to identify individual information brokers;

(B) for each information broker, provides the information described in paragraph (1);

(C) provides links to individual information brokers through which an individual may easily exercise the rights provided under subsection (b) of this Section; and

(D) provides a mechanism by which an individual may, after the Commission has verified the identity of the individual making such request, easily request to all registered information brokers the deletion of all covered information related to such individual. Each information broker must delete the covered information no later than **[**30 days**]** after the request was made.

(d) FTC REGISTRY FEES.—

(1) IN GENERAL.—The Commission shall assess and collect an annual fee pursuant to this section to implement and enforce the central Internet registry of information brokers required under subsection (c) or any other regulation issued by the Commission to carry out this Act.

(2) ANNUAL FEE.—The Commission shall charge each information broker that registers for the central Internet registry of information brokers an annual fee of **[**$15,000**]**.

(3) Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amount specified in paragraph (2) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

[SEC. 11. PROHIBITION ON DISCRIMINATORY USE OF DATA.

(a) DISCRIMINATION IN ECONOMIC OPPORTUNITIES.—

(1) CONDUCT PROHIBITED.—It shall be unlawful for any covered entity to process covered information for the purposes described in paragraph (2) in a manner that discriminates against or makes an economic opportunity unavailable or offered on different terms, on the basis of a person's or class of persons' race, color, religion, national origin, sex, age, or disability.

(2) PURPOSES DESCRIBED.—The purposes referred to in paragraph (1) include advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for housing, employment, credit, insurance, or educational offers or opportunities.

(b) DISCRIMINATION IN PLACES OF PUBLIC ACCOMMODATION.—

(1) IN GENERAL.—It shall be unlawful for a covered entity to process covered information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person's or class of persons' race, color, religion, national origin, sex, age, or disability.

(2) DEFINITION OF PLACE OF PUBLIC ACCOMMODATION.—As used in this subsection, the term "place of public accommodation" means any type of business considered a place of public accommodation pursuant to section 201(b) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(b)) or section 301(7) of the Americans with Disabilities Act of 1990 (42 U.S.C. 12181(7)), and any business that offers goods or services through the Internet to the general public.

(3) INTERFERENCE WITH RIGHTS AND PRIVILEGES—It shall be unlawful for any person to—

(A) withhold, deny, or attempt to withhold or deny, or deprive or attempt to deprive, any person of any right or privilege secured by this subsection; or

(B) intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person with the purpose of interfering with any right or privilege secured by this subsection; or

(C) punish or attempt to punish any person for exercising or attempting to exercise any right or privilege secured by this subsection.

(c) BURDEN OF PROOF.—

(1) If the processing of covered information in a manner or for the purposes described in subsections (a) or (b) causes a disparate impact on the basis of any of the characteristics described in paragraph (a)(1) or (b)(1), the covered entity shall have the burden of demonstrating that—

(A) such processing of data—

(i) is not intentionally discriminatory; and

(ii) is necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; and

(B) there is no reasonable alternative policy or practice that could serve the interest described in clause (ii) of subparagraph (A) with a less discriminatory effect.

(2) RULE OF CONSTRUCTION—When a disparate impact results from a covered entity's processing of covered information by means of automated decision-making, including machine learning or artificial intelligence, the effects of such automated decision-making may be analyzed as a whole without reference to any individual component.

(d) EXCEPTIONS.—Nothing in this section shall limit covered entities from processing covered information for—

(1) the purpose of advertising, marketing, or soliciting economic opportunities to underrepresented populations in a fair, non-deceptive, and non-predatory manner; or

(2) legitimate internal testing or auditing for the purpose of preventing unlawful discrimination or otherwise determining the extent or effectiveness of the covered entity's compliance with this section.

(e) REPORTS TO CONGRESS—Not later than two years after the effective date of this Act, and biennially thereafter, the Commission, in consultation with the Department of Housing and Urban Affairs, the Department of Labor, the Consumer Financial Protection Bureau, the Department of Education, the Department of Health and Human Services, the Department of Veteran Affairs, and the Civil Rights Division of the Department of Justice, shall submit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate concerning violations of this Act and enforcement actions undertaken to resolve such violations, enforcement priorities of the Commission, resources needed by the Commission to implement and enforce this Act, and developments in the state of the art of processing of covered information that may result in discrimination or disparities in—

(1) employment opportunities;

(2) housing opportunities;

(3) access to credit by individuals;

(4) educational opportunities;

(5) health care or health insurance; and

(6) opportunities for veterans.**]**

[SEC. 12. ADDITIONAL PROHIBITIONS.

(a) PROHIBITION ON TAKE-IT-OR-LEAVE-IT—A covered entity shall not condition the provision of a product or service or the quality of customer experience to any individual on an individual's agreement to waive any rights guaranteed by this Act **[**or to the individual's consent to the processing of the individual's covered information other than information necessary to provide the product or service**]**.

(b) PROHIBITION ON FINANCIAL INCENTIVES

(1) IN GENERAL—A covered entity may not offer an individual a financial incentive in exchange for an individual's agreement to waive any rights guaranteed by this Act **[**or to the individual's consent to the processing of the individual's covered information other than information necessary to provide the product or service**]**.

(2) RULES OF CONSTRUCTION—Nothing in subsection (b) shall be construed to—

(A) prohibit the relation of the price of a service or the level of service provided to an individual to the provision, by the individual, of financial information that is necessarily collected and used only for the purpose of initiating, rendering, billing for, or collecting payment for a service or product requested by the individual from the covered entity; or

(B) prohibit a covered entity from offering a loyalty program that provides discounted or free products or services, or other consideration, in exchange for an individual's continued business with the covered entity, provided that such program otherwise complies with the requirements of this Act and any regulations implementing this Act.**]**

SEC. 13. FTC APPROVED COMPLIANCE GUIDELINES—

(a) In General.—

(1) In General—A covered entity that has an **[**annual gross revenue of $25,000,000 or less**],** processes covered information of fewer than **[**50,000**]** individuals, **[**and derives less than 50 percent of its annual revenues from selling consumers' personal information**]** or a group of such covered entities may apply to the Commission for approval of one or more sets of self-regulatory guidelines governing the processing of covered information by a covered entity.

(2) Such application shall include:

(A) a description of how the proposed guidelines will meet or exceed the requirements of this Act;

(B) a description of the entities or activities the proposed guidance is designed to cover;

(C) a list of the covered entities, if any are known at the time of application, that intend to adhere to the guidelines; and

(D) a description of how such covered entities will be independently assessed for compliance with the guidelines and how compliance will be enforced.

(3) COMMISSION REVIEW.—

(A) INITIAL APPROVAL.—

(i) As soon as feasible after the receipt of proposed guidelines submitted pursuant to paragraph (1), the Commission shall provide an opportunity for public comment on such proposed guidelines.

(ii) The Commission shall approve an application regarding proposed guidelines under paragraph (1) if the applicant demonstrates that such guidelines—

(I) meet or exceed requirements of this Act; and

(II) provide for the regular review and validation by an independent organization not associated with the covered entity and approved by the Commission to conduct such reviews of the privacy practices of the covered entity to ensure that the covered entity continues to meet or exceed the requirements of this Act;

(III) include a means of enforcement if the covered entity does not meet or exceed the requirements, which may include referral to the Commission for enforcement consistent with section 15 of this Act.

(iii) Within **[**180 days**]** of receipt, the Commission shall issue a determination approving or denying an application regarding the proposed guidelines submitted pursuant to paragraph (1) and providing its reasons for approving or denying such application.

(B) APPROVAL OF MODIFICATIONS.—

(i) If a covered entity or group of covered entities make material changes to guidelines previously approved by the Commission, the covered entity or group of covered entities must submit the updated guidelines to the Commission for approval.

(ii) The Commission shall approve or deny any material change to the guidelines within **[**90 days**]** after submission for approval by the covered entity or group of covered entities.

(C) WITHDRAWAL OF APPROVAL.—If at any time the Commission determines that the guidelines previously approved no longer meets the requirements of this Act or a regulation promulgated under this Act or that compliance with the approved guidelines are insufficiently enforced by the covered entity or group of such covered entities the Commission shall notify the covered entities or group of such entities its intention to withdraw approval of such guidelines and the basis for doing so. Upon receipt of such notice, the covered entity or group of such entities may cure any alleged deficiency with the guidelines or the enforcement of such guidelines within [90] days. If the covered entity or group of such entities cures and such cures are approved by the Commission, then the Commission may not withdraw approval of such guidelines.

(4) Covered entities that have an **[**annual gross revenue in excess of $25,000,000**],** processes covered information of **[**50,000**]** or more individuals, **[**and derives 50 percent or

more of its annual revenues from selling consumers' personal information**]** are not eligible to participate in guidelines approved under this section.

(5) DEEMED COMPLIANCE.—A covered entity that is eligible to participate in guidelines approved under this section shall be deemed in compliance with this Act if it is in compliance with guidelines approved by the Commission pursuant to this section. If such covered entity is not in compliance with guidelines approved under this section, that covered entity is subject to enforcement under section 15 of this Act.

SEC. 14. BUREAU OF PRIVACY.

(a) ESTABLISHMENT.—The Chairman of the Commission shall establish a new administrative unit in the Commission to be known as the Bureau of Privacy, which shall—

(1) administer and enforce this Act and other consumer privacy or data security laws or regulations within the Commission's jurisdiction;

(2) educate consumers regarding their rights under this Act;

(3) provide guidance to covered entities regarding their obligations under this Act; and

(4) provide support and assistance to small businesses seeking to comply with this Act.

(b) APPOINTMENTS.—

(1) DIRECTOR.—The Chairman of the Commission shall appoint a Director of the Bureau of Privacy.

(2) PERSONNEL.—

(A) IN GENERAL.—The Director of the Bureau of Privacy may, without regard to the civil service laws (including regulations), appoint not less than **[**500**]** certified professionals for the purposes of implementing paragraph (a).

(B) APPOINTMENT OF TECHNOLOGISTS.—In appointing certified professionals under subparagraph (A), the Director of the Bureau of Privacy shall appoint at least **[**25**]** certified technologists.

(C) TECHNOLOGISTS DEFINED.—The term "technologists" means individuals, other than attorneys, with training and expertise regarding the state of the art in information technology, information security, network security, software development, computer science, and other related fields and applications.

(c) OFFICE OF BUSINESS MENTORSHIP.

(1) IN GENERAL.—

(A) The Director of the Bureau of Privacy shall establish within the Bureau an Office of Business Mentorship to provide guidance and consultation to covered entities regarding compliance with this Act.

(B) Covered entities may petition the Commission through this office for tailored guidance as to how to comply with the requirements of this Act.

(2) PERSONNEL.—The Director of the Bureau of Privacy shall assign not less than **[**25**]** employees of the Bureau of Privacy to staff the Office of Business Mentorship, of which **[**15**]** must be certified professionals.

(3) SMALL BUSINESS SUPPORT.—The Director of the Bureau of Privacy shall assign not less than **[**5**]** employees of Office of Business Education to provide additional support to covered entities with fewer than **[**50**]** employees.

(d) RULE OF CONSTRUCTION—No provision of this section shall be construed to limit the authority of the Commission under any other provisions of law.

SEC. 15. ENFORCEMENT.

(a) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) ADDITIONAL VIOLATIONS.—

(A) A violation of a written agreement required under section 8 by a processor or third party pertaining to the processing of covered information shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under Section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(B) It shall be an unfair or deceptive act or practice in violation of section 18(a)(1)(B) of the Federal Trade Commission Act for any covered entity that de-identifies covered information to re-identify, or attempt to re-identify, any information that the covered entity has de-identified.

(3) POWERS OF THE COMMISSION.—

(A) Except as provided in section 17(7), the Commission shall enforce this Act and any regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act, and any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(B) Section 16(a) of the Federal Trade Commission act (15 U.S.C. 56(a)) shall not apply to any civil action to enforce this Act or the regulations promulgated under this Act brought by the Commission, and any appeal of such action.

(4) CIVIL PENALTIES.—

(A) IN GENERAL.—A covered entity that violates this Act shall be subject to a civil penalty in the amount calculated by multiplying the number of violations of this Act by an amount not greater than **[**$45,000**]**. **[**Such penalty shall not exceed [$X].**]**

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in subparagraph (A) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—If the attorney general of a State has reason to believe that any covered entity has violated or is violating this Act or a regulation promulgated under this Act that affects one or more residents of that State, the attorney general of the State may bring a civil action in any appropriate district court of the United States, to—

(A) enjoin further such violation by the defendant;

(B) enforce compliance with this Act or such regulation;

(C) obtain civil penalties in the amount provided for under subsection (a);

(D) obtain other remedies permitted under State law; and

(E) obtain damages, restitution, or other compensation on behalf of residents of the State.

(2) NOTICE.—The attorney general of a State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of the complaint in the action , except in any case in which such prior notice is not feasible, in which case the attorney general shall serve such notice immediately upon instituting such action.

(3) INTERVENTION BY THE FTC.—Upon receiving notice under paragraph (2), the Commission shall have the right—

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein; and

(C) to file petitions for appeal.

(4) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act or a regulation promulgated under this Act, no State attorney general, or official or agency of a State, may bring a separate action under paragraph (1) during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act or a regulation promulgated under this Act that is alleged in the complaint. A State attorney general, or official or agency of a State, may join a civil action for a violation of this Act or regulation promulgated under this Act filed by the Commission.

(5) RULE OF CONSTRUCTION.—For purposes of bringing a civil action under paragraph (3), nothing in this Act shall be construed to prevent the chief law enforcement officer, or official or agency of a State, from exercising the powers conferred on such chief law enforcement officer, official or agency of a State, by the laws of the State to conduct investigations, administer oaths or affirmations, or compel the attendance of witnesses or the production of documentary and other evidence.

(6) ACTIONS BY OTHER STATE OFFICIALS.—

(A) IN GENERAL.—In addition to civil actions brought by attorneys general under paragraph (1), any other officer of a State who is authorized by the State to do so, except for any private person on behalf of the State attorney general, may bring a civil action under paragraph (1), subject to the same requirements and limitations that apply under this subsection to civil actions brought by attorneys general.

(B) SAVINGS PROVISION.—Nothing in this subsection may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

[(c) PRIVATE RIGHT OF ACTION**]**

(d) COMMISSION GUIDANCE.—No guidance issued by the Commission with respect to this Act or consultation provided by the Office of Business Mentorship shall confer any rights on any person, State, or locality, nor shall operate to bind the Commission or any person to the approach recommended in such guidance. In any enforcement action brought pursuant to this section, the Commission shall allege a specific violation the Act and may not base such action on, or execute a consent order based on, practices that are alleged to be inconsistent with any such guidance, unless the practices allegedly violate a provision of this Act.

[(e) RULEMAKING CONSIDERATIONS.— For all regulations the Commission promulgates under this Act, the Commission shall—

(1) consider the feasibility of each regulation;

(2) ensure each regulation is reasonable, flexible, and risk-based for different sizes and practices of covered entities; and

(3) ensure that each regulation protects the privacy of individuals as consistent with the intent of each relevant section.**]**

[SEC. 16. RELATION TO STATE AND OTHER FEDERAL LAWS.**][**PREEMPTION**]**

SEC. 17. DEFINITIONS.

In this Act:

(1) BIOMETRIC INFORMATION.—The term "biometric information" means

(A) any information based on an individual's unique, immutable biological attribute or measurement, including fingerprints, voiceprint, iris or retina scan, facial characteristics, or scan of hand or face geometry, that are used to uniquely and durably authenticate the identity of an individual.

(B) The term "biometric information" does not include writing samples, written signatures, photographs, demographic data or physical descriptions such as height, weight, hair color, or eye color, or biological samples used for scientific testing or screening.

(2) BREACH OF SECURITY.—The term "breach of security" means unauthorized access to, acquisition of, or use of data containing covered information.

(3) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(4) CONSUMER PROFILE.—The term "consumer profile" means any covered information, including covered information resulting from any form of processing of an individual's covered information and inferences drawn from an individual's covered information, used to create a profile about the individual reflecting the individual's preferences, predispositions, behavior, attitudes, intelligence, aptitudes, fitness, abilities, attitudes, interests, reliability, location, movements, or other such characteristics.

(5) CONSUMER SCORE.—The term "consumer score" means a numeric value or a categorization derived from a statistical tool or modeling system used by a covered entity to rate, rank, or segment an individual or to predict an individual's preferences, predispositions, behavior, attitudes, intelligence, aptitudes, fitness, abilities, attitudes, interests, reliability, location, movements, or other such characteristics.

(6) CONTENTS OF COMMUNICATIONS.—The term "contents of communications" means any information concerning the substance, purport, or meaning of a communication.

(7) COVERED ENTITY.—The term "covered entity"—

(A) means any organization, corporation, trust, partnership, estate, cooperative, association, sole proprietorship, unincorporated association, or other entity, over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), that processes covered information;

(B) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers; and

(C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any nonprofit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986.

[(8) COVERED INFORMATION.—

(A) DEFINITION.—The term "covered information"—

(i) means any information about an individual possessed by a covered entity that is linked or reasonably linkable to a specific individual **[**or consumer device;**]** and

(ii) does not include—

(I) information that is processed solely for the purpose of employment of an individual by the individual's employer, including any information regarding an individual that pertains to such individual in his or her capacity as an owner, director, or employee of a partnership, corporation, trust, estate, cooperative, association, or other type of entity;

(II) deidentified information;

[(III) information that is rendered unusable, unreadable, or indecipherable.**]**

[(9) DEIDENTIFIED INFORMATION.— The term "de-identified information" means information for which an entity takes reasonable measures to—

(i) ensure that identifying information has been removed;

(ii) ensure that the information is not reasonably linkable to a specific individual or consumer device;

(ii) Publicly disclose that it will not re-identify such information; and

(iii) Contractually prohibit processors and third parties from attempting to re-identify the information.**]**

(10) DISCLOSURE.—The term "disclose" or "disclosure" means to intentionally or unintentionally release, transfer, sell, disseminate, share, publish, lease, license, make available, allow access, fail to restrict access, or otherwise communicate covered information.

[(11) HEALTH INFORMATION.—The term "health information" means covered information that relates to the physical or mental health or condition of an individual, including genetic data, that—

(A) was created, received, or inferred by a health care provider, health plan, employer, or health care clearinghouse;

(B) was created, received, or inferred by an online health product or service;

(C) relates to the provision of health care as that term is defined in 45 C.F.R. 160.103 to an individual;

(D) was solicited from an individual or a member of the individual's family; or

(E) was inferred for a commercial purpose based on other personal information obtained from or about the individual and where such reference relates to a health condition that reasonable individuals would consider highly sensitive.**]**

[(12) INFORMATION BROKER.—The term "information broker" means—

(A) a covered entity that regularly collects, assembles, or maintains covered information and sells or licenses to a third party or is otherwise compensated for disclosing such information for the third party's own purposes.; and

(B) does not include a commercial entity to the extent that such entity processes information collected by and received from a third party concerning individuals who are current or former customers or employees of the third party to provide benefits for the employees or directly transact business with the customers.**]**

(13) INFORMATION REASONABLY LINKABLE.—The term "information reasonably linkable" means information that can be used on its own, or in combination with other information reasonably accessible to the covered entity or to a **[**processor or**]** third party, to identify a covered person or consumer device.

(14) PARTIES TO COMMUNICATIONS.—The term "parties to communications" means records or logs revealing the sender or recipient or destination of an electronic communication or telephone call. The term does not include information provided by an individual to a covered entity for purposes of establishing or maintaining an account or to communicate with the covered entity regarding the covered entity's products or services.

(15) PRECISE GEOLOCATION INFORMATION.—The term "precise geolocation information" means historical or real-time location information, or inferences drawn from other information, capable of identifying the location of an individual or consumer device with specificity sufficient to identify street level location information or an individual's location within a range of 1,640 feet or less.

(16) PROCESS; PROCESSING.—The term "process" or "processing" means any operation or set of operations which is performed on covered information, whether or not by automated means, including any collection, acquisition, recording, assembly, use, storage, disclosure, inference, analysis, deletion, or modification of covered information.

(17) PROCESSOR.—The term "processor" means organization, corporation, trust, partnership, estate, cooperative, association, sole proprietorship, unincorporated association, or other entity that maintains, processes, or otherwise is permitted access to covered information only on behalf of and at the direction of a

covered entity and only to the extent that such entity is acting on behalf of and at the direction of a covered entity. The term "processor" does not include a third party.

[(18) PSEUDONYMIZED INFORMATION.—The term "pseudonymized information" means information that cannot be reasonably linked to a specific individual or consumer device without additional information that is maintained separately, securely, and with limited access by the covered entity, or a processor acting on behalf of such entity.**]**

(19) PUBLICLY AVAILABLE INFORMATION.—The term "publicly available information" means information that is lawfully made available from Federal, State, or local government records and does not include—

(A) sensitive information; or

(B) information used for a purpose that is not reasonably expected by an individual based on the context or purpose for which the information is maintained and made available in government records.

(20) REASONABLE CONSUMER EXPECTATION.—The term "reasonable consumer expectation" means expected in light of the nature of the individual's interaction with the covered entity or within the individual's existing relationship with the covered entity.

[(21) SELL; SELLS; SELLING.—The term "sell," "sells," or "selling" means to license, trade, provide for monetary compensation, or otherwise monetize covered information.**]**

[(22) SENSITIVE INFORMATION.—

(A) DEFINITION.—The term "sensitive information" means—

(i) health information;

(ii) biometric information;

(iii) precise geolocation information;

(iv) social security numbers;

[(v) information concerning an individual's race, color, religion, national origin, sex, age, or disability;**]**

(v) the contents and parties to communications;

[(vii) audio and video recordings captured through a consumer device;**]**

(viii) online browsing history **[**with respect to sensitive information;**]** and

(vi) financial information, including bank account numbers, credit card numbers, debit card numbers, or insurance policy numbers.**]**

[(B) MODIFIED DEFINITION BY RULEMAKING.—The Commission may promulgate regulations under section 553 of title 5, United States Code, to—

(i) review the definition of "sensitive information" under subparagraph (A) to determine whether such definition should be modified to include additional categories of information; and

(ii) modify such definition to include such additional categories of information if the Commission determines individuals reasonably expect such information to be processed in the same manner as the categories listed in (A).**]**

(23) STATE.—The term "State" means each of the 50 States, the District of Columbia, each commonwealth, territory or possession of the United States, and each federally recognized Indian Tribe.

(24) THIRD PARTY.—The term "third party" means a person, to the extent that such person is not a processor, that accesses or receives covered information from, or discloses covered information to, a covered entity. The term "third party" includes any affiliate of a covered entity.

(25) TRACKING.—The term "tracking" means the act or practice of monitoring, archiving, or logging of the online activities or online behavior of an individual or a consumer device reasonably linkable to an individual.

[SEC. 18. AUTHORIZATION OF APPROPRIATIONS.

AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this Act.**]**

[SEC. 19. EFFECTIVE DATE / The Act will take effect upon enactment with a grace period built in for covered entities to consult with the Commission to ensure compliance with the Act.**]**

SEC. 20. CHILDREN'S PRIVACY [TBD]

[SEC. 21. RELATION TO COMMUNICATIONS ACT**]**

Chairman Wicker's Discussion Draft
The United States Consumer Data Privacy Act

The American economy in the 21st century is increasingly driven by the collection and processing of consumer data. While this has resulted in innovative products, services, and technologies, it has also led to numerous high-profile misuses of data. As a result, consumers have demanded that Congress step in to help protect the privacy of their data.

On November 27, 2019, Chairman Wicker released a staff draft of the United States Data Privacy Act (USCDPA). The draft is informed by over a year of bipartisan negotiations and feedback from consumer advocates, state and local governments, and a number of stakeholders representing many sectors of the economy.

USCDPA would:

- **Establish a national standard** for the protection of consumer data privacy, bringing the United States in line with the European Union and other nations with unified standards and giving consumers strong protections regardless of where in America they live, work, or engage in commerce, both online and offline.
- **Give consumers control over their data**: the ability to know what companies have collected about them and request that it be corrected, deleted, or made portable, and the right to consent to or opt out of data practices in a clear and consistent way.
- **Protect the data of minors** under the age of 16 by requiring the individual or the individual's parent or guardian to provide affirmative express consent (i.e. opt-in consent) before the minor's data can be transferred to a third-party.
- **Require transparency and accountability** on the part of companies who collect and process consumer data, including standards for privacy policies, internal privacy controls, the designation of privacy and data security officers, and a new data broker registry.
- **Combat negative uses of data** by setting standards for data security and supporting efforts to mitigate algorithm bias and digital content forgeries, such as "deep fakes."
- **Provide the Federal Trade Commission with new resources and capabilities** to enforce privacy protections, including through targeted rulemaking authority on key issues and by expanding the Commission's authority to cover non-profits and common carriers.
- **Allow states to protect their citizens** by granting state attorneys general the authority to enforce the provisions of the federal law.
- **Preserve existing federal privacy laws** that have been effective in protecting certain types of consumer data, such as the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. 104-191).

American consumers deserve a strong national standard for the protection of their data, and American companies need certainty in order to continue innovating and competing with the rest of the world. USCDPA is a strong, comprehensive approach to achieving that goal.

HIGH LEVEL SUMMARY OF CANTWELL BILL

SCOPE

- The bill applies to all entities subject to the Federal Trade Commission's (FTC) jurisdiction, including commonly controlled/branded entities. The bill does not appear to apply to common carriers except to the extent such carriers are commonly controlled/branded by a covered entity.

- The bill does not apply to small businesses, defined as entities with $25 million or less in annual revenues, that process the covered data of less than 100,000 consumers per year, and derive less than 50 percent of their revenues from transferring covered data.

- The bill does not preempt the authority of the Federal Communications Commission (FCC) or any other federal agency.

- Compliance with the relevant portions of GLBA, HIPAA/HITECH, FCRA, FERPA and the Social Security Act is deemed to be compliance with this legislation with respect to those laws' privacy and data security provisions.

- The bill only preempts state laws that directly conflict with the new federal law. A conflict does not exist if a state law "affords a greater level of protection to individuals protected under this Act."

SUBSTANTIVE REQUIREMENTS

- As part of its duty of loyalty to consumers, a covered entity is prohibited from engaging in a deceptive or harmful data practice.

    - A deceptive data practice is defined as the processing or transfer of covered data that would constitute a deceptive act or practice in violation of Section 5 of the FTC Act.

    - A harmful data practice would be defined as the processing or transfer of covered data that cause (1) financial, physical or reputational injury; (2) physical or other offensive intrusion into a consumer's private affairs if such intrusion would be offensive to a reasonable person; or (3) other substantial injury to a consumer.

- Covered entities would have to be transparent about their privacy and data security policies, including the categories and specific names of service providers and third parties to which covered data is transferred (and the reason for such transfer) as well as the length of time a covered entity will keep covered data.

- Consumers would have the right to opt-out of transfers of covered data to third parties.

  - Covered data includes information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including information created by the derivation of information, data, assumptions, or conclusions from data about an individual, household, or a device used by an individual or household.

  - Covered data does not include de-identified data, employee data, or public records.

- Consumers would have to opt-in before a covered entity could process or transfer sensitive data that is not publicly available information, except if such processing or transfer is to complete a transaction/fulfill an order/service, ensure the functionality of a service, prevent fraud/malicious activity, comply with a legal obligation, prevent harm, or conduct scientific research.

  - Sensitive covered data includes government-issued identifiers; certain information about an individual's health; financial information; biometric data; precise geolocation information; private communications; an email, address, telephone number, or account log-in credentials; information revealing an individual's race, ethnicity, national origin, religion, or union membership in a manner inconsistent with the individual's reasonable expectation; information revealing an individual's sexual orientation or behavior in a manner inconsistent with an individual's reasonable expectations; information revealing online activities and across third-party websites/online services; calendar/phone log information and photos/videos on an individual's device; private photos/films; and other covered data that the FTC determines to be sensitive pursuant to a rulemaking.

- Consumers would have the right to access, delete, correct inaccuracies about, and export covered data. There is not a limit on the number of times a consumer could assert such rights, which would have to be free of charge.

- A covered entity could only process or transfer covered data for as long as what is reasonably necessary, proportionate, and limited to carry out the specific processing or transfer purpose described in its privacy policy; to carry out a purpose or transfer to which the consumer has opted in; or for certain other permissible operational purposes.

- A covered entity would be required to establish, implement and maintain reasonable data security practices appropriate to the volume and nature of the covered data. Specific requirements include:

  - Assessing vulnerabilities.

  - Preventing and correcting actions.

  - Disposing covered data that is required to be deleted or is no longer necessary for the purpose for which it was collected (unless the consumer has opted into such retention).

  - Training all employees with access to covered data. The FTC, in conjunction with NIST, is required to publish guidance regarding training.

- A covered entity is prohibited from processing or transferring covered data on the basis of race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability:

  - For advertising, marketing or other commercial purposes related to housing, employment, credit or education in a manner that unlawfully discriminates against a consumer or class of consumers; or

  - In a manner that unlawfully segregates, discriminates against, or otherwise makes unavailable to a consumer a place of public accommodation or its goods and services.

- A covered entity that uses algorithmic decision-making to make or facilitate advertising for housing, education, employment, or credit opportunities (or eligibility for such services) would be required to conduct an annual impact assessment.

RULEMAKING AUTHORITY

- The bill provides broad rulemaking authority to the FTC to enforce the bill's substantive requirements and to oversee a covered entity's interaction with service providers and third parties. The bill includes a specific rulemaking on biometric data.

REMEDIES

- The FTC may initiate a suit to enforce the law, and it may seek consumer redress. The bill requires the FTC to create a new bureau to handle implementation of the new law.

- State Attorneys General and Consumer Protection Officers could enforce the federal law.

- The bill includes an explicit private right of action with damages of $100-$1000 per violation per day or actual damages, whichever is greater, as well as punitive damages, attorney's fees, and other relief as the court deems appropriate. Violation of the statute constitutes an injury-in-fact to an individual.

- The bill permits states to adopt a private right of action to enforce the new federal law.

- The bill does not preempt state or federal common law causes of action, or state consumer protection laws.

- The bill would ban pre-dispute arbitration and pre-dispute joint action waivers.

Diane Sacks LLC

December 2019

Privacy and Security Round Up

OCR Stepping Up Enforcement of HIPAA Access Request Violations

On December 12, 2019, the HHS Office for Civil Rights (OCR) announced a settlement of $85,000 against Korunda Medical, LLC for failing to provide access to a patient's medical records as required by HIPAA. Based on the OCR press release and resolution agreement, it appears that the patient repeatedly asked that the records be sent to a third party in electronic format, but Korunda failed to do so in a timely manner or in the required format. It also charged more than a reasonable cost-based fee (presumably for sending a hard copy of the records). In addition to the monetary payment, Korunda agreed to a one-year corrective action plan that included submitting for OCR's approval a policy and procedure for addressing access requests (which is to include its method for calculating how much to charge for labor, supplies and postage for responding to an access request) and workforce training.

Comments: OCR's press release, announcing that this is the second enforcement action under its "Right to Access Initiative", couldn't be clearer that a patient's right to access health records is a top OCR priority. OCR states that it will "vigorously enforce" this right, with the goal of waking up health care providers from their "sleepy bureaucratic inertia." As with many OCR investigations, this one was triggered by an individual complaint, and OCR took enforcement action only after it provided the covered entity with technical assistance regarding its access obligations and the covered entity still failed to comply.

House Energy and Commerce Committee Releases Bipartisan Draft Privacy Bill

On December 18, 2019, House Energy and Commerce Committee staff released a draft bipartisan privacy bill. Described as comprehensive in scope by a Committee spokesman, the bill includes many provisions seen in privacy bills introduced in recent months. These include providing consumers with certain data rights (such as the right to access, correct and delete their information) and requiring covered entities to publish privacy policies, implement data security measures and report breaches to the Federal Trade Commission (FTC). The draft would expand the authority of the FTC to enforce its provisions along with state attorney generals, requiring it to issue privacy regulations covering a range of issues, including limiting how long covered entities may retain personal information. The draft has been circulated to industry stakeholders, with feedback requested by January 24, 2020.

Comments: In order to gain bipartisan support, the draft has placeholders for the two most divisive issues between the parties, namely, federal preemption and a private right of action. Nevertheless, it represents an important first step towards building the necessary support to enact broad-based federal privacy legislation.

California Consumer Privacy Act (CCPA) Developments

The comment period on the proposed regulations issued under the CCPA by the California Attorney General (AG) ended on December 6, 2019. Some of the issues raised by commentators included: concerns about defined terms such as "business", "service provider", "third party", "personal information" and "household"; concern that the law will unfairly disadvantage smaller businesses that do not have the same resources as large companies to comply with the requirements; requests for model notices and disclosures to reduce consumer confusion and reduce compliance costs; questions about data collected by telephone and call recordings, including how to provide notice and what information must be provided in response to requests; and requests for an enforcement delay, at least for small businesses.

Comments: *In an interview on December 10, the AG indicated that his office has no intention of delaying enforcement. However, noting that his office has limited resources to pursue violators, the AG also stated that his office will "look kindly" on those who demonstrate an effort to comply, noting that his office has limited resources to pursue violators. In light of this, businesses have no choice but to comply with their best understanding of the CCPA's requirements, at least until final regulations are issued.*

U.S Department of Education (DOE) and OCR Issue Joint Guidance on Privacy of Student Records

On December 19, 2019, the DOE and OCR issued joint guidance on the applicability of the Family Educational Rights and Privacy Act (FERPA) and HIPAA to student records. This guidance, which updates guidance issued in November 2008, is extensive, including 27 FAQs. It explains when each law applies, where the two laws may intersect, and that the two laws generally do not overlap, since the definition of "protected health information" (PHI) under HIPAA explicitly excludes education and treatment records covered by FERPA. The guidance make clear that records covered by HIPAA or FERPA may generally be shared with family, caregivers, and even law enforcement, in situations involving a danger to the student or others.

Comments: As with HIPAA guidance issued in 2017 at the height of the opioid crisis, the thrust of the guidance is to dispel the misconception that mental health records held by covered entities may not be disclosed without the individual's permission even in emergencies or other situations in which the individual or others are at risk. While this is correct with respect to FERPA and HIPAA, the guidance does not mention that state laws and 42 CFR Part 2 may be considerably more restrictive, and it is often a concern about these laws, rather than HIPAA or FERPA, that causes health care providers to withhold mental health information.

Cures 2.0 "Call to Action" Comments Raise Privacy Issues

In response to a request from Reps. Diana DeGette (D-CO) and Fred Upton (R-MI) in November asking for input on items to include in follow-up legislation to the 21st Century Cures Act (so-called "Cures 2.0"), several groups have raised privacy concerns, particularly with respect to third-party application programming interfaces (APIs). Echoing concerns raised about the proposed interoperability rule issued by the HHS Office of the National Coordinator for Health IT (ONC), provider groups, such as the American Hospital Association, and health IT groups, such as the College of Healthcare Information Management Executives (CHIME), expressed concerns about APIs gaining access to patient information without being held to the same privacy or security standards as HIPAA entities. Other groups have suggested that HIPAA be modernized and broadened to cover health data that currently falls outside its ambit, and for a harmonization of federal privacy laws, particularly HIPAA and 42 CFR Part 2. Yet others, including PhRMA and academic medical centers, emphasized the need for increased interoperability, patient access to data, and patient-centric digital tools.

Comments: As with the comments on ONC's proposed interoperability rule, the suggestions for health data issues to address in Cures 2.0 reflect not only the varying priorities of different stakeholders, but also the inherent tension in maintaining patient privacy while making health information more accessible to patients, providers and researchers.

Data Breach Class Actions

In court documents filed in Arizona in early December, Banner Health agreed to pay class members up to $6 million for costs resulting from a 2016 hacking attack in which the records of 2.9 million individuals was compromised. Banner Health also agreed to provide affected individuals with two years of credit monitoring and identity protection services, and to improve its data security. When notifying affected individuals of the incident in 2016, Banner Health had offered one year of free credit and identity monitoring services, but the plaintiffs in the class action argued that this was inadequate, noting that at least one plaintiff had fraudulent bank accounts opened and tax returns filed in her name. This settlement was followed by a decision of the Georgia Supreme Court on December 23, 2019 allowing a negligence lawsuit to proceed for another 2016 hacking attack where the victims' data was offered for sale on the dark net. Overturning the lower court decision, the Georgia Supreme Court found that the fact that the data was actively stolen by a criminal enterprise and placed on the web for sale made the risk of harm more than speculative in nature, thereby allowing the negligence claim to proceed.

Comments: The cases illustrate that when there is evidence of criminal activity and intent in a data breach, courts are likely to view the risk of harm as substantial enough to constitute an injury warranting compensation.

Please contact Diane Sacks at dsacks@sacksllc.com or (202)459-2101 for more information on any of these items. This newsletter is intended to provide general information only and is not intended as legal advice.