

[DISCUSSION DRAFT]

FEBRUARY 16, 2018

115TH CONGRESS  
2D SESSION

**H. R.** \_\_\_\_\_

To [be provided]

---

IN THE HOUSE OF REPRESENTATIVES

Mr. LUETKEMEYER (for himself and Mrs. CAROLYN B. MALONEY of New York) introduced the following bill; which was referred to the Committee on \_\_\_\_\_

---

**A BILL**

To [be provided]

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Data Acquisition and  
5 Technology Accountability and Security Act”.

6 **SEC. 2. DEFINITIONS.**

7 For purposes of this Act, the following definitions  
8 apply:

1           (1) AFFILIATE.—The term “affiliate” means  
2 any company that controls, is controlled by, or is  
3 under common control with another company

4           (2) AGENCY.—The term “agency” has the same  
5 meaning as in section 551(1) of title 5, United  
6 States Code.

7           (3) BREACH OF DATA SECURITY.—The term  
8 “breach of data security” means the unauthorized  
9 acquisition of personal information from a covered  
10 entity, but does not include the good faith acquisi-  
11 tion of personal information by an employee or agent  
12 of the entity, if the personal information is not used  
13 or subject to further unauthorized acquisition.

14           (4) COMMISSION.—The term “Commission”  
15 means the Federal Trade Commission.

16           (5) CONSUMER.—The term “consumer” means  
17 an individual.

18           (6) CONSUMER REPORTING AGENCY THAT COM-  
19 PILES AND MAINTAINS FILES ON CONSUMERS ON A  
20 NATIONWIDE BASIS.—The term “consumer reporting  
21 agency that compiles and maintains files on con-  
22 sumers on a nationwide basis” has the same mean-  
23 ing as in section 603(p) of the Fair Credit Report-  
24 ing Act (15 U.S.C. 1681a(p)).

1           (7) COVERED ENTITY.—The term “covered en-  
2           tity” means any person, partnership, corporation,  
3           trust, estate, cooperative, association, or other entity  
4           that accesses, maintains, or stores personal, or han-  
5           dles personal information. For purposes of section 3,  
6           a covered entity includes a Federal agency.

7           (8) FINANCIAL INSTITUTION.—The term “fi-  
8           nancial institution” has the same meaning as in sec-  
9           tion 509(3) of the Gramm-Leach-Bliley Act (15  
10          U.S.C. 6809(3)).

11          (9) NON-PROFIT ORGANIZATION.—The term  
12          “non-profit organization” means an organization  
13          that is described in section 501(c)(3) of the Internal  
14          Revenue Code of 1986 and exempt from tax under  
15          section 501(a) of such Code. Such term shall not in-  
16          clude a credit union as defined in section 101 of the  
17          Federal Credit Union Act. (12 U.S.C. 1752).

18          (10) PERSONAL INFORMATION.—

19                 (A) IN GENERAL.—The term “personal in-  
20                 formation” means an individual’s first name or  
21                 initial and last name in combination with any  
22                 one of the following data elements:

23                         (i) A non-truncated Social Security  
24                         number, driver’s license number, passport  
25                         number, alien registration number, or

1 other government-issued unique identifica-  
2 tion number.

3 (ii) A financial account number, alone  
4 or in combination with its security code,  
5 access code, or password that enables an  
6 individual to obtain credit, withdraw funds,  
7 or engage in a financial transaction.

8 (iii) Automatic measurements of bio-  
9 metric data unique to an individual that is  
10 required to authenticate an individual's  
11 identity to complete a financial trans-  
12 action.

13 (iv) A user name in combination with  
14 any associated security code, access code,  
15 or password that is required for an indi-  
16 vidual to obtain money, or purchase goods,  
17 services, or any other thing of value.

18 (B) EXCEPTIONS.—The term “personal in-  
19 formation” does not include—

20 (i) information that is rendered unus-  
21 able, unreadable, or indecipherable; or

22 (ii) information available from a pub-  
23 licly available source, including information  
24 obtained from a news report, periodical, or  
25 other widely distributed media, or from

1 Federal, State, or local government  
2 records.

3 (11) THIRD PARTY.—

4 (A) IN GENERAL.—The term “third party”  
5 means any entity that processes, maintains,  
6 stores, or handles, or otherwise is permitted ac-  
7 cess to personal information in connection with  
8 providing services to a covered entity.

9 (B) EXCEPTION.—The term “third party”  
10 does not include a service provider.

11 (12) SERVICE PROVIDER.—The term “service  
12 provider” means any entity subject to the Commu-  
13 nications Act of 1934 (47 U.S.C. 151 et seq.) that  
14 provides electronic data transmission, routing, inter-  
15 mediate and transient storage, or connections to its  
16 system or network, where such entity providing such  
17 service does not select or modify the content of the  
18 electronic data, is not the sender of the intended re-  
19 cipient of the data, and does not differentiate per-  
20 sonal information from other information that such  
21 entity transmits, routes, stores, or for which such  
22 entity provides connections. Any such entity shall be  
23 treated as a service provider under this Act only to  
24 the extent that it is engaged in the provision of such

1 transmission, routing, intermediate and transient  
2 storage, or connections.

3 **SEC. 3. PROTECTION OF INFORMATION.**

4 (a) SECURITY SAFEGUARDS REQUIRED.—

5 (1) IN GENERAL.—Each covered entity shall de-  
6 velop, implement, and maintain administrative, tech-  
7 nical, and physical safeguards that are reasonably  
8 designed to protect the security and confidentiality  
9 of personal information from unauthorized acquisi-  
10 tion that is reasonably likely to result in identity  
11 theft, fraud, or economic loss.

12 (2) FLEXIBILITY OF SAFEGUARDS.—A covered  
13 entity's safeguards under paragraph (1) shall be ap-  
14 propriate to—

15 (A) the size and complexity of the covered  
16 entity;

17 (B) the nature and scope of the activities  
18 of the covered entity;

19 (C) the cost of available tools to improve  
20 security and reduce vulnerabilities; and

21 (D) the sensitivity of the personal informa-  
22 tion maintained by the covered entity.

23 (3) ELEMENTS.—As part of its reasonable safe-  
24 guards, a covered entity shall—

1 (A) designate an owner, officer, employee,  
2 or employees to maintain safeguards;

3 (B) identify material internal and external  
4 risks to the security and confidentiality of per-  
5 sonal information and assess the sufficiency of  
6 any safeguards in place to control these risks,  
7 including consideration of risks in each relevant  
8 area of the covered entity's operations, such  
9 as—

10 (i) employee training and manage-  
11 ment;

12 (ii) information systems, including  
13 network and software design, as well as in-  
14 formation processing, storage, trans-  
15 mission, and disposal; and

16 (iii) detecting, preventing and re-  
17 sponding to attacks, intrusions, or other  
18 systems failures;

19 (C) implement safeguards designed to con-  
20 trol the risks identified in its risk assessment,  
21 and regularly assess the effectiveness of those  
22 safeguards;

23 (D) maintain reasonable procedures for the  
24 security of personal information by third parties  
25 to require that such third parties maintain rea-

1           sonable administrative, technical, and physical  
2           safeguards designed to protect the security and  
3           confidentiality of such information; and

4                   (E) evaluate the safeguards and make rea-  
5           sonable adjustments to these safeguards in light  
6           of any material changes in technology, internal  
7           or external threats to personal information, and  
8           the covered entity's own changing business ar-  
9           rangements or operations.

10          (b) ADMINISTRATIVE REQUIREMENT.—If a covered  
11       entity has a board of directors, the covered entity shall  
12       report to its board or an appropriate committee of the  
13       board at least annually, including describing the overall  
14       status of the safeguards and the covered entity's compli-  
15       ance with this Act.

16       **SEC. 4. NOTIFICATION OF BREACH OF DATA SECURITY.**

17          (a) PRELIMINARY INVESTIGATION REQUIRED.—If a  
18       covered entity believes that a breach of data security con-  
19       taining personal information may have occurred, the cov-  
20       ered entity shall conduct an immediate investigation to—

- 21                   (1) assess the nature and scope of the incident;  
22                   (2) identify any personal information that may  
23       have been involved in the incident;



1           (3) determine if the personal information has or  
2           is likely to have been acquired without authorization;  
3           and

4           (4) take reasonable measures to restore the se-  
5           curity and confidentiality of the systems com-  
6           promised in the breach of data security.

7           (b) NOTICE REQUIRED.—

8           (1) IN GENERAL.—If, after completion of the  
9           preliminary investigation under subsection (a), a  
10          covered entity determines that there is a reasonable  
11          risk that the breach of data security has resulted in  
12          or will result in identity theft, fraud, or economic  
13          loss to the consumers to whom the personal informa-  
14          tion involved in the incident relates, the covered enti-  
15          ty shall immediately notify without unreasonable  
16          delay—

17                 (A) the Secret Service or the Federal Bu-  
18                 reau of Investigation, if the breach of data se-  
19                 curity involves personal information relating to  
20                 5,000 or more consumers;

21                 (B) the appropriate agency or authority  
22                 defined in section 5, if the breach of data secu-  
23                 rity involves personal information relating to  
24                 5,000 or more consumers;

1 (C) if the breach of data security involves  
2 payment card numbers, any relevant payment  
3 card network, if the breach of data security in-  
4 volves personal information relating to more  
5 than 5,000 or more consumers; and

6 (D) each consumer reporting agency that  
7 compiles and maintains files on consumers on a  
8 nationwide basis, if the breach of data security  
9 involves personal information relating to 5,000  
10 or more consumers.

11 (2) CONSUMER NOTIFICATION.—If a covered  
12 entity determines after completion of the preliminary  
13 investigation under subsection (a) that there is a  
14 reasonable risk that the breach of data security has  
15 resulted in identity theft, fraud, or economic loss to  
16 any consumer, the covered entity shall immediately  
17 notify such consumer, without unreasonable delay  
18 except under circumstances outlined in paragraph  
19 (5).

20 (3) FORM OF NOTIFICATION.—Notification to  
21 consumers under paragraph (2) shall be provided  
22 by—

- 23 (A) written notification;  
24 (B) telephonic notification;  
25 (C) email notification; or

1 (D) substitute notification made available  
2 through a link on the home page of the covered  
3 entity's website and broadcast media in the  
4 States where the consumers reside, if providing  
5 written, telephonic, or email notification is not  
6 feasible due to lack of sufficient contact infor-  
7 mation for the majority of consumers that the  
8 entity is required to notify.

9 (4) CONTENT OF NOTIFICATION.—The informa-  
10 tion contained in the notification to consumers  
11 under paragraph (2) shall be maintained by the cov-  
12 ered entity and made available to consumers upon  
13 request for not less than six months and shall in-  
14 clude—

15 (A) a description of the type of personal  
16 information maintained by the covered entity  
17 that was involved in the breach of data security;

18 (B) a description of the actions taken by  
19 the covered entity to restore the security and  
20 confidentiality of the personal information in-  
21 volved in the breach of data security; and

22 (C) a description of steps a consumer can  
23 take to protect themselves from identity theft.

24 (5) DELAY REQUIRED WHEN REQUESTED BY  
25 LAW ENFORCEMENT.—A covered entity shall delay

1 any notification described under paragraph (2) if  
2 such delay is requested by the Secret Service, the  
3 Federal Bureau of Investigation, or State law en-  
4 forcement. The covered entity shall notify pursuant  
5 to such paragraph when the Secret Service, the Fed-  
6 eral Bureau of Investigation, or State law enforce-  
7 ment, as applicable, determines that notification is  
8 permitted.

9 (c) REQUIREMENTS OF THIRD PARTIES.—

10 (1) REQUIREMENTS.—If a third party becomes  
11 aware that a breach of data security involving data  
12 in electronic form containing personal information  
13 that is maintained or otherwise handled on behalf of  
14 a covered entity has or may have occurred, the third  
15 party shall—

16 (A) investigate the nature and scope of the  
17 suspected breach of data security;

18 (B) promptly notify the covered entity  
19 whose data has or may have been compromised;

20 (C) cooperate with the covered entity by  
21 providing sufficient information about the sus-  
22 pected breach of data security to allow the cov-  
23 ered entity to meet its obligations under this  
24 section. That cooperation shall include informa-  
25 tion , but need not be limited to—

1 (i) informing the covered entity of the  
2 suspected breach of data security, includ-  
3 ing giving notice of the date or approxi-  
4 mate date of the breach of data security  
5 and the nature of the breach of data secu-  
6 rity; and

7 (ii) informing the covered entity of  
8 any steps the third party has taken or  
9 plans to take relating to the suspected  
10 breach of data security; and

11 (D) notify any other person as has been  
12 previously agreed to in a writing signed by the  
13 third party and the covered entity.

14 (2) RULES OF CONSTRUCTION.—

15 (A) Nothing in this subsection shall be  
16 construed to interfere with the right of a cov-  
17 ered entity and third party to agree in writing  
18 regarding their respective obligations to provide  
19 notice under this section.

20 (B) Nothing in subparagraph (C) of para-  
21 graph (1) shall be interpreted to require a third  
22 party to disclose confidential business informa-  
23 tion or trade secrets to a covered entity.

24 (d) REQUIREMENTS OF SERVICE PROVIDERS.—

1           (1) REQUIREMENTS.—If a service provider be-  
2 comes aware of a breach of data security involving  
3 data in electronic form containing personal informa-  
4 tion that is owned or licensed by a covered entity  
5 that connects to or uses a system or network pro-  
6 vided by the service provider for the purpose of  
7 transmitting, routing, or providing intermediate or  
8 transient storage of such data, such service provider  
9 shall notify the covered entity that initiated such  
10 connection, transmission, routing, or storage of the  
11 data containing personal information breached if  
12 such covered entity can be reasonably identified. If  
13 a service provider is acting solely as a service pro-  
14 vider for purposes of this subsection, the service pro-  
15 vider has no other obligations under this section.

16           (2) RULE OF CONSTRUCTION.—Nothing in this  
17 subsection shall be construed to prohibit a service  
18 provider from being considered for purposes of this  
19 Act as a covered entity for the purposes of informa-  
20 tion it collects as a first party.

21           (e) COMMUNICATIONS WITH FINANCIAL ACCOUNT  
22 HOLDERS.—

23           (1) GENERALLY.—If a covered entity experi-  
24 ences a breach of data security involving personal in-  
25 formation, a financial institution that holds an ac-

1 count to which the personal information relates may  
2 communicate with the account holder regarding the  
3 breach, including—

4 (A) an explanation that the financial insti-  
5 tution was not breached, and that the breach  
6 occurred at a covered entity that had access to  
7 the consumer's personal information; and

8 (B) identify the covered entity that experi-  
9 enced the breach after the covered entity has  
10 provided notice required by subsection (b)(2).

11 (2) RULE OF CONSTRUCTION.—Nothing in this  
12 subsection shall be construed as creating an obliga-  
13 tion on a financial institution to provide notice to  
14 consumers.

15 (f) NOTIFICATION FOR CHANGE OF ONLINE AC-  
16 COUNT CREDENTIALS.—In the case of a breach of data  
17 security involving personal information for an online ac-  
18 count, and no other personal information, the covered enti-  
19 ty may comply with this section by providing the notifica-  
20 tion in electronic or other form that directs the person  
21 whose personal information has been breached promptly  
22 to change his or her security code, access code, or pass-  
23 word as applicable to protect the online account with the  
24 covered entity.

1 **SEC. 5. ENFORCEMENT.**

2 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-  
3 MISSION.—

4 (1) ENFORCEMENT PRACTICES.—A violation of  
5 section 3 or 4 shall be enforced in the same manner  
6 as a violation of a rule prescribed under section  
7 18(a)(1)(B) of the Federal Trade Commission Act  
8 (15 U.S.C. 57a(a)(1)(B)).

9 (2) POWERS OF COMMISSION.—The Commis-  
10 sion shall enforce this Act in the same manner, by  
11 the same means, and with the same jurisdiction,  
12 powers, and duties as though all applicable terms  
13 and provisions of the Federal Trade Commission Act  
14 (15 U.S.C. 41 et seq.) were incorporated into and  
15 made a part of this Act, and any covered entity sub-  
16 ject to the Commission's authority who violates this  
17 Act shall be subject to the penalties and entitled to  
18 the privileges and immunities provided in the Fed-  
19 eral Trade Commission Act.

20 (3) JURISDICTION.—

21 (A) Notwithstanding section 5(a)(2) of the  
22 Federal Trade Commission Act (15 U.S.C.  
23 45(a)(2)), the Commission shall have authority  
24 over common carriers subject to the Commu-  
25 nications Act of 1934 (47 U.S.C. 151 et seq.)  
26 to enforce this Act.



1 (B) Notwithstanding any jurisdictional  
2 limitation of the Federal Trade Commission  
3 Act, the Commission shall have authority over  
4 any nonprofit organization to enforce this Act.

5 (4) PENALTY FACTORS.—In determining the  
6 amount of a civil penalty, the degree of culpability,  
7 any history of prior such conduct, ability to pay, ef-  
8 fect on ability to continue to do business, proactive  
9 security measures taken, material harm to con-  
10 sumers, and the overall economics of covered entity  
11 such as annual number of customers, revenue or em-  
12 ployees, and such other matters as justice may re-  
13 quire shall be taken into account.

14 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-  
15 ERAL.—

16 (1) CIVIL ACTION.—With respect to a covered  
17 entity that is not a financial institution, in any case  
18 in which the attorney general of a State has reason  
19 to believe that an interest of the residents of that  
20 State has been or is threatened or adversely affected  
21 by any covered entity that violates section 3 or 4 of  
22 this Act, the attorney general of the State, as *parens*  
23 *patriae*, may bring a civil action on behalf of the  
24 residents of the State in a district court of the  
25 United States of appropriate jurisdiction to—

1 (A) enjoin further violation of such section  
2 by the defendant;

3 (B) compel compliance with such section;

4 or

5 (C) obtain civil penalties in the amount de-  
6 termined in the same manner as subsection (a).

7 (2) CONSOLIDATION OF ACTIONS BROUGHT BY  
8 TWO OR MORE STATE ATTORNEYS GENERAL.—  
9 Whenever a civil action under this subsection is  
10 pending and another civil action or actions are com-  
11 menced pursuant to this subsection in a different  
12 Federal district court or courts that involve one or  
13 more common questions of fact, such action or ac-  
14 tions shall be transferred for the purposes of consoli-  
15 dated pretrial proceedings and trial to the United  
16 States District Court for the District of Columbia.  
17 No such actions shall be transferred if pretrial pro-  
18 ceedings in that action have been concluded before  
19 a subsequent action is filed by a State attorney gen-  
20 eral.

21 (3) INTERVENTION BY THE FEDERAL TRADE  
22 COMMISSION.—

23 (A) NOTICE AND INTERVENTION.—In all  
24 cases, the attorney general of a State shall pro-  
25 vide prior written notice of any action under

1 paragraph (1) to the Commission and provide  
2 the Commission with a copy of its complaint,  
3 except in any case which such prior notice is  
4 not feasible, in which case such attorney gen-  
5 eral shall serve such notice immediately upon  
6 instituting such action. The Commission shall  
7 have the right—

- 8 (i) to intervene in the action;  
9 (ii) upon so intervening, to be heard  
10 on all matters arising therein; and  
11 (iii) to file for petitions of appeal.

12 (B) PENDING PROCEEDINGS.—If the Fed-  
13 eral Trade Commission initiates a Federal civil  
14 action for a violation of this Act, no State at-  
15 torney general may bring an action for a viola-  
16 tion of this Act that resulted from the same or  
17 related acts or omissions against a defendant  
18 named in the civil action initiated by the Fed-  
19 eral Trade Commission. If the Federal Trade  
20 Commission has instituted or intervened in a  
21 proceeding or a civil action for a violation of  
22 this Act, no State attorney general may bring  
23 an action under this subsection against any cov-  
24 ered entity named as a defendant in such civil

1           action for any violation of this Act alleged in  
2           the complaint.

3           (4) CONSTRUCTION.—For purposes of bringing  
4           any civil action under paragraph (1), nothing in this  
5           Act shall be construed to prevent an attorney gen-  
6           eral of a State from exercising the powers conferred  
7           on the attorney general by the laws of that State  
8           to—

9                   (A) conduct investigations;

10                   (B) administer oaths or affirmations; or

11                   (C) compel the attendance of witnesses or  
12           the production of documentary and other evi-  
13           dence.

14           (5) LIMITATION.—An attorney general of a  
15           State may not bring an action under this subsection  
16           against any covered entity that is a financial institu-  
17           tion, or its affiliates.

18           (c) ENFORCEMENT FOR FINANCIAL INSTITUTIONS.—  
19           Subject to subsection (e) and notwithstanding any other  
20           provisions of law, sections 3 and 4 shall be enforced exclu-  
21           sively under section 501(b) of the Gramm-Leach-Bliley  
22           Act (15 U.S.C. 6801(b)) by each agency or authority with  
23           authority to enforce section 501(b), with respect to any  
24           financial institution or subsidiary of a financial institution

1 that is subject to the jurisdiction of such agency or author-  
2 ity pursuant to section 501(b).

3 (d) INSURANCE.—This Act shall not apply to any  
4 person engaged in providing insurance.

5 (e) COMPLIANCE.—

6 (1) FINANCIAL INSTITUTIONS.—A covered enti-  
7 ty that is a financial institution shall be deemed to  
8 be in compliance with sections 3 and 4, if the finan-  
9 cial institution—

10 (A) maintains policies and procedures to  
11 protect the confidentiality and security of per-  
12 sonal information that are consistent with the  
13 policies and procedures of the financial institu-  
14 tion that are designed to comply with the re-  
15 quirements of section 501(b) of the Gramm-  
16 Leach-Bliley Act (15 U.S.C. 6801(b)) and any  
17 regulations or guidance prescribed under that  
18 section that are applicable to the financial insti-  
19 tution;

20 (B) is an affiliate of a bank holding com-  
21 pany, bank, or savings and loan holding com-  
22 pany that maintains policies and procedures to  
23 investigate and provide notice to consumers of  
24 breaches of data security that are consistent  
25 with the policies and procedures of a bank or

1 savings association that is an affiliate of the fi-  
2 nancial institution, and the policies and proce-  
3 dures of the bank or savings association are de-  
4 signed to comply with the investigation and no-  
5 tice requirements established by regulations or  
6 guidance under section 501(b) of the Gramm-  
7 Leach-Bliley Act (15 U.S.C. 6801(b)) that are  
8 applicable to the bank holding company or  
9 bank, or savings and loan holding company or  
10 savings association; and

11 (C) provides services that are subject to  
12 regulation and examination by a Federal bank-  
13 ing agency under the Bank Services Company  
14 Act (12 U.S.C. 1861 et seq.) to the extent such  
15 services are subject by contract to breach notifi-  
16 cation obligations imposed by financial institu-  
17 tions in contracts pursuant to Federal banking  
18 agency guidance.

19 (2) OTHER COVERED ENTITIES.—A covered en-  
20 tity shall be deemed to be in compliance with sec-  
21 tions 3 and 4—

22 (A) if the entity is a covered entity for  
23 purposes of the regulations promulgated under  
24 section 264(c) of the Health Insurance Port-  
25 ability and Accountability Act of 1996 (41

1 U.S.C. 1320d-2 note), to the extent that the en-  
2 tity is in compliance with such regulations and  
3 to the extent of the personal information is pro-  
4 tected by such Act; or

5 (B) if the entity is in compliance with sec-  
6 tions 13402 and 13407 of the HITECH Act  
7 (42 U.S.C. 17932; 17937), to the extent the  
8 personal information is protected by such Act.

9 **SEC. 6. RELATION TO STATE LAW.**

10 This Act preempts any law, rule, regulation, require-  
11 ment, standard, or other provision having the force and  
12 effect of law of any State, or political subdivision of a  
13 State, with respect to securing information from unau-  
14 thorized access or acquisition, including notification of un-  
15 authorized access or acquisition of data, except as applica-  
16 ble to any person engaged in providing insurance.

17 **SEC. 7. RELATION TO OTHER LAWS.**

18 (a) [\_\_\_\_].—Notwithstanding any other provision of  
19 law, the Federal Communications Commission shall have  
20 no authority to apply any regulations to covered entities  
21 with respect to securing information from unauthorized  
22 access and acquisition, including notification of unauthor-  
23 ized access and acquisition to data, unless such regula-  
24 tions pertain solely to 9–1–1 calls.

1           (b) **RULE OF CONSTRUCTION.**—Nothing in this sec-  
2 tion otherwise limits the Federal Communication Commis-  
3 sion’s authority with respect to sections 201, 202, 222,  
4 338, and 631 of the Communications Act of 1934 (47  
5 U.S.C. 201, 202, 222, 338, and 551).

6           (c) **PRESERVATION OF COMMISSION AUTHORITY.**—  
7 Nothing in this Act may be construed in any way to limit  
8 or affect the Commission’s authority under any other pro-  
9 vision of law.

10 **SEC. 8. EFFECTIVE DATE.**

11           This Act shall take effect 18 months after the date  
12 of the enactment of this Act.