

105TH CONGRESS
1ST SESSION

H. R. 2937

To provide for the recognition of digital and other forms of authentication as an alternative to existing paper-based methods, to improve efficiency and soundness of the Nation's capital markets and the payment system, and to define and harmonize the practices, customs, and uses applicable to the conduct of electronic authentication, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 8, 1997

Mr. BAKER (for himself and Mr. DREIER) introduced the following bill; which was referred to the Committee on Commerce, and in addition to the Committees on Government Reform and Oversight, the Judiciary, Science, and Banking and Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To provide for the recognition of digital and other forms of authentication as an alternative to existing paper-based methods, to improve efficiency and soundness of the Nation's capital markets and the payment system, and to define and harmonize the practices, customs, and uses applicable to the conduct of electronic authentication, and for other purposes.

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

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Electronic Financial
3 Services Efficiency Act of 1997”.

4 **SEC. 2. FINDINGS AND PURPOSE.**

5 (a) FINDINGS.—The Congress finds the following:

6 (1) In recent years, new technological applica-
7 tions have had a significant impact on bank capital
8 markets and the manner in which business enter-
9 prises and financial institutions conduct their activi-
10 ties and operations.

11 (2) Financial and consumer transactions and
12 communications are being conducted in digital elec-
13 tronic formats because of the adoption of new tech-
14 nological applications which allow for the instantane-
15 ous retrieval and transmission of information and
16 the electronic consummation of business and per-
17 sonal transactions.

18 (3) These changes relate not only to the cre-
19 ation, retention, and delivery of documentation and
20 other data, but also to the purchase and sale of
21 goods and services, the receipt and payment of
22 funds, and other aspects of commerce and finance.—

23 (4) These developments have allowed for the
24 emergence of a new electronic commerce infrastruc-
25 ture for consumer and financial communications and

1 transactions, and the concomitant emergence of elec-
2 tronic authentication methodologies.

3 (5) These new technologies have impacted, and
4 will continue to impact, the national payment sys-
5 tem, our financial services industry, and our Na-
6 tion's capital markets.

7 (6) Parties to consumer and financial trans-
8 actions have heretofore entered into agreements,
9 consistent with paper-based authentication meth-
10 odologies.

11 (7) Thus, where the formation of agreements
12 are otherwise valid and effective under applicable
13 law, the parties should be able to use electronic au-
14 thentication methodologies of equal or greater reli-
15 ability.

16 (8) Given the size and importance of our do-
17 mestic economy and the fact that electronic com-
18 merce is not limited by geographical or national
19 boundaries and will have a significant impact on
20 international finance, the United States should be
21 actively involved in the development of uniform glob-
22 al standards for electronic authentication.

23 (9) There are many industries that have the
24 technical expertise, can meet proposed national
25 standards, and have the desire to offer electronic au-

1 authentication services. Therefore, it is important not
2 to prematurely limit market access and stifle growth
3 by narrowly defining industries that may provide
4 electronic authentication services.

5 (10) As a result, it is appropriate for Congress
6 to enable a framework whereby government, busi-
7 ness enterprises, financial institutions, and consum-
8 ers can participate in electronic commerce in a via-
9 ble, safe, efficient, and consistent manner.

10 (b) PURPOSE.—The purpose of this Act is to provide
11 for the recognition of digital and other forms of authen-
12 tication as an alternative to existing paper-based methods,
13 to improve efficiency and soundness of the Nation’s capital
14 markets and payment system, and to define and har-
15 monize the practices, customs, and uses applicable to the
16 conduct of electronic authentication.

17 **SEC. 3. DEFINITIONS.**

18 For purposes of this Act, the following definitions
19 shall apply:

20 (1) ELECTRONIC COMMERCE.—The term “elec-
21 tronic commerce” means the transaction or conduct
22 of business in whole or part by electronic means.

23 (2) ELECTRONIC MEANS.—The term “electronic
24 means” includes all forms of electronic communica-
25 tion mediated by computer, including telephonic

1 communications, facsimile, electronic mail, electronic
2 data exchanges, satellite, cable, and fiber optic com-
3 munications.

4 (3) ELECTRONIC AUTHENTICATION.—The term
5 “electronic authentication” means any methodology,
6 technology, or technique intended to—

7 (A) establish the identity of the maker,
8 sender, or originator of a document or commu-
9 nication in electronic commerce; and

10 (B) establish the fact that the document or
11 communication has not been altered.

12 (4) DIGITAL SIGNATURE.—The term “digital
13 signature” means any electronic symbol or series of
14 symbols, created, or processed by a computer, in-
15 tended by the party using it (or authorizing its use)
16 to have the same legal force and effect as a manual
17 signature.

18 (5) CERTIFICATION AUTHORITY.—The term
19 “certification authority” means any private or public
20 entity which provides assurance that a particular
21 digital signature, or other form of electronic authen-
22 tication, is tied to the identity of an individual or
23 legal entity, or attests to the current validity of such
24 a signature.

1 (6) TRUSTED THIRD PARTY.—The term “trust-
2 ed third party” means a certification authority who
3 is known to 2 transacting parties and whose certifi-
4 cate is relied upon by those parties.

5 (7) CERTIFICATE.—The term “certificate” is an
6 electronic message the contents of which enable the
7 recipient to determine the attestation made regard-
8 ing the certificate holder by the certification author-
9 ity.

10 (8) STATE.—The term “State” has the mean-
11 ing given to such term in section 3 of the Federal
12 Deposit Insurance Act.

13 (9) AFFILIATE.—The term “affiliate” means
14 any person that controls, is controlled by, or is
15 under common control with another person.

16 **SEC. 4. COMMUNICATIONS WITH FEDERAL GOVERN-**
17 **MENTAL AGENCIES.**

18 In any written communication with an agency, de-
19 partment, or instrumentality of the United States Govern-
20 ment, or with any court of the United States, in which
21 a signature is required or used, any party to the commu-
22 nication may affix a signature by use of a digital signature
23 with a certificate issued by a trusted third party.

1 **SEC. 5. VALIDITY OF ELECTRONIC AUTHENTICATION.**

2 (a) VALIDITY OF ELECTRONIC COMMUNICATIONS
3 WITH AGENCIES, COURTS, AND INSTRUMENTALITIES OF
4 THE UNITED STATES.—All forms of electronic authentica-
5 tion that comport with standards as described in sub-
6 sections (a) and (b) of section 6 of this Act shall have
7 standing equal to paper-based, written signatures, such
8 that, with respect to any communications with Federal ad-
9 ministrative agencies, Federal courts and other instrumen-
10 talities of the United States government—

11 (1) any rule of law which requires a record to
12 be in writing shall be deemed satisfied; and

13 (2) any rule of law which requires a signature
14 shall be deemed satisfied.

15 (b) VALIDITY OF ELECTRONIC COMMUNICATIONS IN
16 GENERAL.—Unless otherwise expressly prohibited by the
17 laws of any State, all forms of electronic authentication
18 that comport with the standards as described in sub-
19 sections (a) and (b) of section 6 shall have standing equal
20 to paper-based, written signatures, such that—

21 (1) any rule of law which requires a record to
22 be in writing shall be deemed satisfied; and

23 (2) any rule of law which requires a signature
24 shall be deemed satisfied.—

1 **SEC. 6. CRITERIA FOR ELIGIBILITY.**

2 (a) **ELECTRONIC AUTHENTICATION.**—Electronic au-
3 thentication technology shall be deemed valid hereunder
4 if such technology—

5 (1) reliably establishes the identity of the
6 maker, sender, or originator of a document or com-
7 munication in electronic commerce; and

8 (2) reliably establishes the fact that the docu-
9 ment or communication has not been altered.

10 (b) **EMERGING TECHNOLOGIES.**—2 currently ac-
11 knowledged signature technologies are public key cryptog-
12 raphy and signature dynamics technology. In contempla-
13 tion of acceptance of other technological applications, the
14 following criteria shall be applied in the determination of
15 their validity for purposes of this Act:

16 (1) The identification methodology shall be
17 unique to the person making, sending, originating a
18 document or communication.

19 (2) The identification technology shall be capa-
20 ble of verification.

21 (3) The identification method or device shall be
22 under the sole control of the person using it

23 (4) The identification technology or device shall
24 be linked to data or communication transmitted in
25 such a manner that if such data or communication
26 has been altered, the authentication becomes invalid.

1 **SEC. 7. NATIONAL ASSOCIATION OF CERTIFICATION AU-**
2 **THORITIES.**

3 (a) IN GENERAL.—There is hereby established the
4 National Association of Certification Authorities (here-
5 after in this section referred to as the “Association”).

6 (b) REGISTRATION.—Any person or group wishing to
7 provide electronic authentication services in the United
8 States shall be a registered member of the Association.

9 (c) DENIAL OF MEMBERSHIP.—

10 (1) DECERTIFICATION.—The Association may
11 deny membership to any person or group (or any af-
12 filiate of such person or group) who has been decer-
13 tified pursuant to subsection (e)(5)(D)(iii).

14 (2) FAILURE TO COMPLY WITH CODE OF CON-
15 DUCT.—The Association may deny membership to
16 any provider of electronic authentication services
17 who fails to comply with any guidelines, standards,
18 or codes of conduct regarding the use of electronic
19 authentication established by the Electronic Authen-
20 tications Standards Review Committee pursuant to
21 subsection (e)(2).

22 (3) FAILURE TO MEET STANDARDS.—The Asso-
23 ciation may deny membership to any provider of
24 electronic authentication services to any person or
25 group that is unable to meet standards established
26 pursuant to subsections (a) and (b) of section 6.

1 (4) PRACTICES INCONSISTENT WITH THIS
2 ACT.—The Association may bar an individual from
3 becoming affiliated with a member of the Association
4 if such individual has engaged in acts or practices
5 inconsistent with this Act and rules established by
6 the Association.

7 (5) LACK OF COOPERATION.—The Association
8 may bar any person or group from becoming affili-
9 ated with a member if such person or group does
10 not agree—

11 (A) to supply the Association with such in-
12 formation with respect to the relationship and
13 dealings of such person or group with the mem-
14 ber as may be specified in the rules of the Asso-
15 ciation; and

16 (B) to permit examination of the books
17 and records of such person or group to verify
18 the accuracy of any information so supplied.

19 (d) DUES.—The rules of the Association shall provide
20 for the equitable allocation of reasonable dues, fees, and
21 other charges among members and other persons applying
22 for membership or using any facility or system which the
23 Association operates or controls.

24 (e) STANDARDS REVIEW COMMITTEE.—

1 (1) IN GENERAL.—The Association shall estab-
2 lish the Electronic Authentications Standards Re-
3 view Committee (hereafter in this subsection re-
4 ferred to as the “Standards Review Committee”)
5 which shall establish, develop, and refine criteria to
6 be applied to the emerging electronic authentication
7 industry, including—

8 (A) the roles and responsibilities of the
9 parties involved in electronic authentication;

10 (B) the application of the standards de-
11 scribed in section 6(b) to emerging electronic
12 authentication;

13 (C) recognition of foreign legal and regu-
14 latory standards; and

15 (D) transparency requirements, licensing,
16 and registration of certification authorities.

17 (2) RULEMAKING.—With the approval of the
18 Secretary of the Treasury, the Standards Review
19 Committee shall establish and adopt such guidelines,
20 standards, and codes of conduct regarding the use of
21 electronic authentication by members of the Associa-
22 tion, including the rights and responsibilities of cer-
23 tification authorities in matters involving notifica-
24 tion, disclosure requirements, liability of consumers
25 and certification authorities, and hearing procedures

1 regarding disciplinary actions taken by the Stand-
2 ards Review Committee in furtherance of the pur-
3 poses of this Act.

4 (3) ENFORCEMENT.—The Standards Review
5 Committee shall have enforcement powers to ensure
6 minimum standards and protections for consumers
7 and shall establish and adopt disciplinary procedures
8 and policies in furtherance of the purposes of this
9 Act.

10 (4) DISCIPLINARY ACTIONS.—The Standards
11 Review Committee shall organize in a manner such
12 that disciplinary actions against members shall be
13 heard fairly and in a timely fashion and afford due
14 process.

15 (5) NOTIFICATION.—

16 (A) IN GENERAL.—If, in the opinion of the
17 Standards Review Committee, any certification
18 authority is engaging or has engaged in conduct
19 in contravention of any guideline, standard, or
20 code of conduct prescribed in accordance with
21 paragraph (3), the Standards Review Commit-
22 tee shall notify such certification authority.

23 (B) STATEMENT OF FACTS.—The notifica-
24 tion shall contain a statement of the facts con-
25 stituting the violation.

1 (C) PERIOD FOR RESPONSE.—The certifi-
2 cation authority shall respond to such notifica-
3 tion within 15 days.

4 (D) SANCTIONS.—Based upon the re-
5 sponse of the certification authority, if the
6 Standards Review Committee determines that
7 the certification authority has violated any such
8 guideline, standard, or code of conduct, the
9 committee may take any of the following ac-
10 tions:

11 (i) CENSURE.—Publicly censure the
12 certification authority.

13 (ii) SUSPENSION.—Prohibit the cer-
14 tification authority from providing elec-
15 tronic authentication services in the United
16 States for such period of time as the com-
17 mittee may determine to be appropriate.

18 (iii) DECERTIFICATION.—Prohibit the
19 certification authority from providing elec-
20 tronic authentication services in the United
21 States.

22 (iv) CIVIL PENALTY.—Impose mone-
23 tary penalties on the certification author-
24 ity.

1 (6) JUDICIAL REVIEW.—Any party aggrieved by
2 an order of the Standards Review Committee under
3 this Act may obtain a review of such order in the
4 United States Court of Appeals within any circuit
5 wherein such party has its principal place of busi-
6 ness or in the court of Appeals in the District of Co-
7 lumbia, by filing in the court, within 30 days after
8 the entry of the Standards Review Committee order,
9 a petition praying that the order of the Standards
10 Review Committee be set aside. A copy of such peti-
11 tion shall be forthwith transmitted to the Standards
12 Review Committee by the clerk of the court, and
13 thereupon the Standards Review Committee shall
14 file in the court the record made before the Stand-
15 ards Review Committee. Upon the filing of such pe-
16 tition the court shall have the jurisdiction to affirm,
17 set aside, or modify the order of the Standards Re-
18 view Committee and to require the Standards Re-
19 view Committee to take such action with regard to
20 the matter under review as the court deems proper.
21 The findings of the Standards Review Committee as
22 to the facts, if supported by substantial evidence,
23 shall be conclusive.—

24 (7) REPORT TO SECRETARY OF THE TREAS-
25 URY.—The Standards Review Committee shall

1 transmit to the Secretary of the Treasury, not later
2 than February 20 and July 20 of each year, com-
3 plete reports of the activities of the committee un-
4 dertaken in furtherance of the purposes of this Act,
5 including a statement of the committee's objectives
6 and plans for the next semiannual reporting period.

7 (8) STUDIES AND RECOMMENDATIONS.—The
8 Standards Review Committee may conduct studies
9 to carry out the purposes of this Act. On the basis
10 of such studies the Committee may make rec-
11 ommendations to the Secretary of the Treasury con-
12 cerning the implementation of this Act and such leg-
13 islative and administrative action as the committee
14 may determine to be necessary to promote the rec-
15 ognition of electronic authentication as an alter-
16 native to paper-based methods of verification.

17 **SEC. 8. OVERSIGHT.**

18 The Secretary of the Treasury shall provide effective
19 oversight and shall review the activities of the Electronic
20 Authentication Standards Review Committee on a semi-
21 annual basis, providing a venue for the discussion and air-
22 ing of all activity, standards and other material issues
23 which may have arisen during that time period.

1 **SEC. 9. CONSUMER PROTECTION.**

2 (a) IN GENERAL.—No provision of this Act shall be
3 construed as impairing any right afforded a consumer
4 under the provisions of any law applicable to an underly-
5 ing transaction or communication that is authenticated by
6 digital signature or other form of electronic authentication
7 that comports with the standards as described in sub-
8 sections (a) and (b) of section 6.

9 (b) NOTIFICATION.—Any transaction or communica-
10 tion involving a consumer that is authenticated by digital
11 signature or other form of electronic authentication that
12 comports with the standards as described in subsections
13 (a) and (b) of section 6 shall contain a notification of the
14 fact that such transaction or communication has been au-
15 thenticated. Such notification shall be in such form as pre-
16 scribed by the Electronic Authentication Standards Re-
17 view Committee.

18 (c) DEFINITIONS.—For purposes of this section, the
19 following definitions shall apply:

20 (1) CONSUMER.—The term “consumer” means
21 an individual.

22 (2) TRANSACTION.—The term “transaction” re-
23 fers only to transactions for personal, family, or
24 household purposes.

1 (3) COMMUNICATION.—The term “communica-
2 tion” means a communication pertaining only to
3 personal, family, or household purposes.

○