

108TH CONGRESS
2D SESSION

S. 2472

To require that notices to consumers of health and financial services include information on the outsourcing of sensitive personal information abroad, to require relevant Federal agencies to prescribe regulations to ensure the privacy and security of sensitive personal information outsourced abroad, to establish requirements for foreign call centers, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MAY 20, 2004

Mr. NELSON of Florida introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To require that notices to consumers of health and financial services include information on the outsourcing of sensitive personal information abroad, to require relevant Federal agencies to prescribe regulations to ensure the privacy and security of sensitive personal information outsourced abroad, to establish requirements for foreign call centers, 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 “Increasing Notice of
3 Foreign Outsourcing Act”.

4 **SEC. 2. HEALTH PRIVACY.**

5 (a) FOREIGN-BASED BUSINESS ASSOCIATE.—In this
6 section, the term “foreign-based business associate”
7 means a business associate, as defined under the regula-
8 tions promulgated pursuant to section 264(c) of the
9 Health Insurance Portability and Accountability Act of
10 1996 (42 U.S.C. 1320d–2 note), whose operation is based
11 outside the United States and that receives protected
12 health information and processes such information outside
13 the United States.

14 (b) NOTICES.—

15 (1) IN GENERAL.—The Secretary of Health and
16 Human Services (referred to in this section as the
17 “Secretary”) shall revise the regulations prescribed
18 pursuant to section 264(c) of the Health Insurance
19 Portability and Accountability Act of 1996 (42
20 U.S.C. 1320d–2 note) to require a covered entity (as
21 defined under such regulations and referred to in
22 this section as a “covered entity”), that outsources
23 protected health information (as defined under such
24 regulations and referred to in this section as “pro-
25 tected health information”), outside the United

1 States to include in such entity's notice of privacy
2 protections the following:

3 (A) The following information in simple
4 language:

5 (i) Notification that the covered entity
6 outsources protected health information to
7 foreign-based business associates.

8 (ii) Any risks and consequences to the
9 privacy and security of protected health in-
10 formation that arise as a result of the
11 processing of such information outside the
12 United States.

13 (iii) Additional measures the covered
14 entity is taking to protect the protected
15 health information outsourced for proc-
16 essing outside the United States.

17 (B) A certification that the covered entity
18 has taken reasonable steps to ensure that the
19 handling of protected health information will be
20 done in compliance with applicable laws in all
21 instances where protected health information is
22 processed outside the United States, including
23 the reasons for the certification.

24 (2) EFFECTIVE DATE.—A covered entity shall
25 be required to include in such entity's notice of pri-

1 vacy protections the information and certification de-
2 scribed in paragraph (1) for notices issued on or
3 after the date on which the Secretary prescribes reg-
4 ulations pursuant to this section or the date that is
5 365 days after the date of enactment of this Act,
6 whichever date is earlier. Nothing in this subsection
7 shall be construed to require a covered entity to re-
8 issue notices issued before the date on which the
9 Secretary prescribes regulations pursuant to this
10 section or the date that is 365 days after the date
11 of enactment of this Act, whichever date is earlier,
12 to include in such notices the information and cer-
13 tification described in paragraph (1).

14 (c) RULEMAKING.—

15 (1) IN GENERAL.—

16 (A) REGULATORY AUTHORITY.—The Sec-
17 retary shall—

18 (i) prescribe such regulations con-
19 sistent with paragraph (2) as may be nec-
20 essary to carry out this section with re-
21 spect to foreign outsourcing; and

22 (ii) determine the appropriate pen-
23 alties to impose upon a covered entity for
24 a violation of a provision of this subsection
25 or subsection (b).

1 (B) PROCEDURES AND DEADLINES.—The
 2 regulations described in subparagraph (A) shall
 3 be prescribed in accordance with all applicable
 4 legal requirements and shall be issued in final
 5 form not later than 365 days after the date of
 6 enactment of this Act.

7 (2) NECESSARY REGULATIONS.—The Secretary
 8 shall prescribe regulations—

9 (A) requiring that a contract between a
 10 covered entity and such entity’s foreign-based
 11 business associate contain a provision that pro-
 12 vides such entity with the right to audit such
 13 associate, as needed, to monitor performance
 14 under the contract; and

15 (B) requiring that foreign-based business
 16 associates and subcontractors of covered enti-
 17 ties be contractually bound by Federal privacy
 18 standards and security safeguards.

19 (d) BREACH OF SECURITY.—

20 (1) BREACH OF SECURITY OF THE SYSTEM.—

21 In this subsection, the term “breach of security of
 22 the system”—

23 (A) means the compromise of the security,
 24 confidentiality, or integrity of computerized
 25 data that results in, or there is a reasonable

1 basis to conclude has resulted in, the unauthor-
2 ized acquisition of and access to protected
3 health information maintained by the covered
4 entity, foreign-based business associate, or sub-
5 contractor; and

6 (B) does not include good faith acquisition
7 of protected health information by an employee
8 or agent of the covered entity, foreign-based
9 business associate, or subcontractor for the pur-
10 poses of the entity, associate, or subcontractor,
11 if the protected health information is not used
12 or subject to further unauthorized disclosure.

13 (2) DATABASE SECURITY.—

14 (A) COVERED ENTITY.—A covered enti-
15 ty—

16 (i) that owns or licenses electronic
17 data containing protected health informa-
18 tion shall, following the discovery of a
19 breach of security of the system containing
20 such data, notify the Secretary of such
21 breach; or

22 (ii) that receives a notification under
23 subparagraph (B) of a breach, shall notify
24 the Secretary of such breach.

25 (B) OTHER PARTIES.—

1 (i) THIRD PARTY.—The Secretary
2 shall require that a contract between a cov-
3 ered entity and such entity’s foreign-based
4 business associate contain a provision that
5 if the foreign-based business associate (or
6 any subcontractor of such associate) owns
7 or licenses electronic data containing pro-
8 tected health information that was pro-
9 vided to the associate through the covered
10 entity, the associate (or subcontractor)
11 shall, following the discovery of a breach of
12 security of the system containing such
13 data—

14 (I) notify the entity from which it
15 received the protected health informa-
16 tion of such breach; and

17 (II) provide a description to the
18 entity from which it received the pro-
19 tected health information of any cor-
20 rective actions taken to guard against
21 future security breaches.

22 (ii) NOTIFICATION PROCESS.—Each
23 entity that receives a notification under
24 clause (i) shall notify the entity from which
25 it received the protected health information

1 of such breach until the notification
 2 reaches the foreign-based business asso-
 3 ciate who shall, in turn, notify the covered
 4 entity of such breach.

5 (C) TIMELINESS OF NOTIFICATION.—All
 6 notifications required under subparagraphs (A)
 7 and (B) shall be made as expediently as pos-
 8 sible and without unreasonable delay fol-
 9 lowing—

10 (i) the discovery of a breach of secu-
 11 rity of the system; and

12 (ii) any measures necessary to deter-
 13 mine the scope of the breach, prevent fur-
 14 ther disclosures, and restore the reasonable
 15 integrity of the data system.

16 (3) EFFECTIVE DATE.—This subsection shall
 17 take effect on the expiration of the date that is 365
 18 days after the date of enactment of this subsection.

19 **SEC. 3. FINANCIAL PRIVACY.**

20 (a) FOREIGN-BASED BUSINESS.—Section 509 of the
 21 Gramm-Leach-Bliley Act (15 U.S.C. 6809) is amended by
 22 adding at the end the following:

23 “(12) FOREIGN-BASED BUSINESS.—The term
 24 ‘foreign-based business’ means a nonaffiliated third
 25 party whose operation is based outside the United

1 States and that receives nonpublic personal informa-
 2 tion and processes such information outside the
 3 United States.”.

4 (b) FINANCIAL NOTICES.—

5 (1) IN GENERAL.—Section 503(b) of the
 6 Gramm-Leach-Bliley Act (15 U.S.C. 6803(b)) is
 7 amended—

8 (A) in paragraph (3), by striking “and”
 9 after the semicolon;

10 (B) in paragraph (4), by striking the pe-
 11 riod at the end and inserting “; and”; and

12 (C) by adding at the end the following:

13 “(5) if the financial institution outsources non-
 14 public personal information outside the United
 15 States—

16 “(A) information informing the consumer
 17 in simple language—

18 “(i) that the financial institution
 19 outsources nonpublic personal information
 20 to foreign-based businesses;

21 “(ii) of any risks and consequences to
 22 the privacy and security of an individual’s
 23 nonpublic personal information that arise
 24 as a result of the processing of such infor-
 25 mation outside the United States; and

1 “(iii) of the additional measures the
2 financial institution is taking to protect the
3 nonpublic personal information outsourced
4 for processing outside the United States;
5 and

6 “(B) a certification that the financial insti-
7 tution has taken reasonable steps to ensure that
8 the handling of nonpublic personal information
9 will be done in compliance with applicable laws
10 in all instances where nonpublic personal infor-
11 mation is processed outside the United States,
12 including the reasons for the certification.”.

13 (2) EFFECTIVE DATE.—A financial institution
14 shall include in such institution’s disclosure the in-
15 formation and certification described in the amend-
16 ment made by paragraph (1)(C) for disclosures pro-
17 vided on or after the date on which the regulatory
18 agency that has jurisdiction over such institution
19 pursuant to section 505 of the Gramm-Leach-Bliley
20 Act (15 U.S.C. 6805) prescribes regulations pursu-
21 ant to the amendments made by this section or the
22 date that is 365 days after the date of enactment of
23 this Act, whichever date is earlier. Nothing in this
24 subsection, or the amendments made by this sub-
25 section, shall be construed to require a financial in-

1 stitution to reissue disclosures provided before the
 2 date on which the regulatory agency that has juris-
 3 diction over such institution pursuant to section 505
 4 of the Gramm-Leach-Bliley Act (15 U.S.C. 6805)
 5 prescribes regulations pursuant to the amendments
 6 made by this section or the date that is 365 days
 7 after the date of enactment of this Act, whichever
 8 date is earlier, to include in such disclosures the in-
 9 formation and certification described in the amend-
 10 ment made by paragraph (1)(C).

11 (c) RULEMAKING.—Section 504 of the Gramm-
 12 Leach-Bliley Act (15 U.S.C. 6804) is amended by adding
 13 at the end the following:

14 “(c) RULEMAKING ON FOREIGN OUTSOURCING.—

15 “(1) IN GENERAL.—

16 “(A) REGULATORY AUTHORITY.—The Fed-
 17 eral banking agencies, the National Credit
 18 Union Administration, the Secretary of the
 19 Treasury, the Securities and Exchange Com-
 20 mission, and the Federal Trade Commission
 21 (referred to in this subsection as the ‘regulatory
 22 agencies’) shall—

23 “(i) prescribe such regulations con-
 24 sistent with paragraph (2) as may be nec-
 25 essary to carry out this subtitle with re-

1 spect to foreign outsourcing, with respect
 2 to the financial institutions subject to their
 3 jurisdiction under section 505; and

4 “(ii) determine the appropriate pen-
 5 alties to impose upon financial institutions
 6 for a violation of a provision of this sub-
 7 section.

8 “(B) COORDINATION, CONSISTENCY, AND
 9 COMPARABILITY.—The regulatory agencies shall
 10 consult and coordinate with each other for the
 11 purposes of assuring, to the extent possible,
 12 that the regulations prescribed by each such
 13 agency are consistent and comparable with the
 14 regulations prescribed by the other such agen-
 15 cies.

16 “(C) PROCEDURES AND DEADLINES.—The
 17 regulations described in subparagraph (A) shall
 18 be prescribed in accordance with all applicable
 19 legal requirements and shall be issued in final
 20 form not later than 365 days after the date of
 21 enactment of this subsection.

22 “(2) NECESSARY REGULATIONS.—The regu-
 23 latory agencies shall prescribe regulations—

24 “(A) requiring that a contract between a
 25 financial institution and such institution’s for-

1 eign-based business contain a provision that
 2 provides such institution with the right to audit
 3 such business, as needed, to monitor perform-
 4 ance under the contract; and

5 “(B) requiring that foreign-based busi-
 6 nesses and subcontractors of financial institu-
 7 tions be contractually bound by Federal privacy
 8 standards and security safeguards.”.

9 (d) BREACH OF SECURITY.—Section 502 of the
 10 Gramm-Leach-Bliley Act (15 U.S.C. 6802) is amended by
 11 adding at the end the following:

12 “(f) BREACH OF SECURITY.—

13 “(1) BREACH OF SECURITY OF THE SYSTEM.—

14 In this subsection, the term ‘breach of security of
 15 the system’—

16 “(A) means the compromise of the secu-
 17 rity, confidentiality, or integrity of computer-
 18 ized data that results in, or there is a reason-
 19 able basis to conclude has resulted in, the unau-
 20 thorized acquisition of and access to nonpublic
 21 personal information maintained by the finan-
 22 cial institution, foreign-based business, or sub-
 23 contractor; and

24 “(B) does not include good faith acquisi-
 25 tion of nonpublic personal information by an

1 employee or agent of the financial institution,
2 foreign-based business, or subcontractor for the
3 purposes of the institution, business, or subcon-
4 tractor, if the nonpublic personal information is
5 not used or subject to further unauthorized dis-
6 closure.

7 “(2) DATABASE SECURITY.—

8 “(A) FINANCIAL INSTITUTION.—A finan-
9 cial institution—

10 “(i) that owns or licenses electronic
11 data containing nonpublic personal infor-
12 mation shall, following the discovery of a
13 breach of security of the system containing
14 such data, notify the entity under which
15 the institution is subject to jurisdiction
16 under section 505 of such breach; or

17 “(ii) that receives a notification under
18 subparagraph (B) of a breach, shall notify
19 the entity under which the institution is
20 subject to jurisdiction under section 505 of
21 such breach.

22 “(B) OTHER PARTIES.—

23 “(i) IN GENERAL.—The Federal bank-
24 ing agencies, the National Credit Union
25 Administration, the Secretary of the Treas-

1 ury, the Securities and Exchange Commis-
2 sion, and the Federal Trade Commission
3 shall require, with respect to the financial
4 institutions subject to their jurisdiction
5 under section 505, that a contract between
6 a financial institution and such institu-
7 tion’s foreign-based business contain a pro-
8 vision that if the foreign-based business (or
9 any subcontractor of such business) owns
10 or licenses electronic data containing non-
11 public personal information that was pro-
12 vided to the business through the financial
13 institution, the business (or subcontractor)
14 shall, following the discovery of a breach of
15 security of the system containing such
16 data—

17 “(I) notify the entity from which
18 it received the nonpublic personal in-
19 formation of such breach; and

20 “(II) provide a description to the
21 entity from which it received the non-
22 public personal information of any
23 corrective actions taken to guard
24 against future security breaches.

1 “(ii) NOTIFICATION PROCESS.—Each
 2 entity that receives a notification under
 3 clause (i) shall notify the entity from which
 4 it received the nonpublic personal informa-
 5 tion of such breach until the notification
 6 reaches the foreign-based business who
 7 shall, in turn, notify the financial institu-
 8 tion of such breach.

9 “(C) TIMELINESS OF NOTIFICATION.—All
 10 notifications required under subparagraphs (A)
 11 and (B) shall be made as expeditiously as pos-
 12 sible and without unreasonable delay fol-
 13 lowing—

14 “(i) the discovery of a breach of secu-
 15 rity of the system; and

16 “(ii) any measures necessary to deter-
 17 mine the scope of the breach, prevent fur-
 18 ther disclosures, and restore the reasonable
 19 integrity of the data system.

20 “(3) EFFECTIVE DATE.—This subsection shall
 21 take effect on the expiration of the date that is 365
 22 days after the date of enactment of this sub-
 23 section.”.

1 **SEC. 4. FOREIGN CALL CENTERS.**

2 (a) FOREIGN CALL CENTER DEFINED.—In this sec-
3 tion, the term “foreign call center” means a foreign-based
4 service provider or a foreign-based subcontractor of such
5 provider that—

6 (1) is unaffiliated with the entity that utilizes
7 such provider or subcontractor; and

8 (2) provides customer-based service and sales or
9 technical assistance and expertise to individuals lo-
10 cated in the United States via the telephone, the
11 Internet, or other telecommunications and informa-
12 tion technology.

13 (b) REQUIREMENT.—A contract between a foreign
14 call center and an entity that utilizes such foreign call cen-
15 ter to initiate telephone calls to, or receive telephone calls
16 from, individuals shall include a requirement that each
17 employee of the foreign call center disclose the physical
18 location of such employee upon the request of such indi-
19 vidual.

20 (c) CERTIFICATION REQUIREMENT.—An entity de-
21 scribed in subsection (b) shall submit an annual certifi-
22 cation to the Federal Trade Commission on whether or
23 not the entity and its subsidiaries, and the foreign call
24 center employees and its subsidiaries, have complied with
25 subsection (b). Such annual certifications shall be made
26 available to the public.

1 (d) NONCOMPLIANCE.—An entity described in sub-
2 section (b) or its subsidiaries that violates subsection (b)
3 shall be subject to such civil penalties as the Federal
4 Trade Commission prescribes under subsection (e).

5 (e) REGULATIONS.—Not later than 365 days after
6 the date of enactment of this Act, the Federal Trade Com-
7 mission shall prescribe such regulations as are necessary
8 for effective monitoring and compliance with this section.
9 Such regulations shall include appropriate civil penalties
10 for noncompliance with this section.

○