SECTION-BY-SECTION ANALYSIS

Section 1. Short Title.

This section would provide that the legislation be cited as the "Identity Theft Protection Act."

Section 2. Protection of Sensitive Personal Information.

Section 2 would require within 1 year the Federal Trade Commission (FTC) to promulgate regulations that would: (1) require covered entities develop, implement, and maintain appropriate safeguards to protect sensitive personal information; (2) take into account technological remedies such as encryption or truncation to use in these safeguards; (3) require procedures for credentialing third parties seeking access to sensitive personal information; and (4) require disposal procedures for entities covered under this Act.

Section 3. Notification of Security Breach Risk.

Section 3 would require a covered entity that suffers a breach of security and determines that the breach affects the sensitive personal information of 1,000 or more individuals to report the breach to the FTC or other appropriate regulating agencies and notify all consumer reporting agencies. The FTC would be required to post a report of breach notifications received without disclosing any sensitive personal information or names of the individuals affected.

In addition, if a covered entity has a basis for concluding that a reasonable risk of identity theft exists for 1 or more individuals, the covered entity would be required to notify every individual for whom the breach of security affected.

Section 3(2)(c) would require within 1 year after the enactment of the Act that the FTC promulgate regulations that establish methods of notification to be followed by covered entities in complying with the Act. The FTC would be required to take into consideration the types of information involved, the nature and scope of the security breach, and the most effective means of notification to individuals.

Section 3 also would require a covered entity to give notice to consumers in the most expedient manner possible, but not later than 90 days following the discovery by the covered entity of a breach, unless a Federal law enforcement agency determines that the timely giving of notice would materially impede a Federal civil or criminal investigation, or threaten Federal national security or homeland security.

Section 4. Security Freeze.

Section 4 would allow a consumer to place a security freeze on his or her credit report by making a request in writing or by telephone to a consumer credit reporting agency. The security freeze would prevent a consumer's credit report from being released to a third party without authorization from the consumer.

A consumer credit reporting agency would be required to notify all other consumer reporting agencies of the request and treat it as though the consumer credit reporting agency received the request form the consumer directly. A consumer credit reporting agency would have up to 5 days after receiving a written request to place a security freeze and 3 days to lift a freeze permanently or for a temporary period. This Act would not prevent a consumer reporting agency from charging a reasonable fee to a consumer for placing or removing a security freeze on his or her credit report unless the consumer was the victim of identity theft and provides the consumer credit reporting agency with a police report at the time of placing a freeze.

The removal of a security freeze would only be allowed upon the request of the consumer or the consumer's credit report was frozen due to a material misrepresentation of fact. The consumer credit reporting agency would be required to notify the customer in writing prior to lifting the freeze if doing so due to a material misrepresentation of fact. If a consumer requests that a security freeze be lifted after providing proper identification, the consumer reporting agency must lift the freeze within 3 days.

Section 4 would require that a consumer reporting agency disclose to the consumer the process of placing and removing a security freeze and explain to the consumer the potential consequences of placing a security freeze.

Section 4 would not apply to the use of a consumer credit report for the following:

- A person or entity with which the consumer has had a prior business relationship for the purpose of reviewing an account or collecting the financial obligation owing from an account or contract.

- Any Federal, State or local agency, law enforcement agency, trial court, or private collection agency acting pursuant to a court order, warrant, or subpoena.

- The Department of Heath and Human Services or any similar State agency acting to investigate Medicare or Medicaid fraud.

- The Internal Revenue Service or a State municipal taxing authority to investigate or collect delinquent taxes or unpaid court orders or any of their other statutory responsibilities.

- The use of consumer credit information for prescreening.

- Any person administering a credit file monitoring subscription to which the consumer has subscribed.

- Any person or entity for the purpose of providing a consumer with his or her credit report or credit score at the consumer's request.

- A check services or fraud prevention services company, which issues reports on incidents of fraud.

- A deposit account information service company, which issues report regarding account closures due to fraud, substantial overdrafts, or similar negative information.

Section (4)(l)(1) would also exempt consumer reporting agencies that act only as a reseller of credit information by assembling and merging information contained in the data base of another consumer credit reporting agency, and does not maintain a permanent data base of credit information from which new consumer reports are produced.

Section 5. Enforcement.

FTC Enforcement: Section 5 would provide that violations of this Act be enforced by the FTC as if they were unfair or deceptive acts or practices proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

Other Agencies: Section 5 would also provide that compliance with the Act be enforced by other agencies under the following laws (see text for United States Code cites):

- The Federal Deposit Insurance Act (for national banks, foreign banks, commercial lenders, bank holding companies, and savings associations);

- The Federal Credit Union Act (for credit unions); and

- The Securities Exchange Act of 1934 (for brokers and dealers)

In event of unauthorized access to consumers' sensitive personal information, Section 5 would allow the FTC to obtain a civil penalty of $11,000 for each individual; and $11,000,000 in the aggregate for all individuals effected by the security breach.

This section would also provide that nothing in this Act establishes a private cause of action against a covered entity for the violation of any provision in this Act. But nothing would affect a consumer's right to bring a civil action that is not under this Act in state or federal court.

In addition, any person to whom title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) applies shall be deemed in compliance with the notification requirements of this Act if that person is deemed compliant with the notification requirements of the Gramm-Leach-Bliley Act.

Section 6. Enforcement of State Attorneys General.

Section 6 would allow States to bring an action under this Act in federal court on behalf of its residents. The State would be required to notify the FTC or the appropriate federal regulator prior to bringing the action, and the FTC or appropriate federal regulator would have the authority to intervene in the action once commenced.

Section 7. Preemption of State Law.

Section 7 of this Act would preempt any State or local law that requires, or holds liable, a covered entity to safeguard sensitive personal information, notify individuals of breaches of security regarding their sensitive personal information, or allow a consumer to place a security freeze on his or her credit report.

Section 8. Social Security Number Protection.

Section 8 would prohibit the solicitation of social security numbers from individuals where there is no specific purpose and which no other identifying number reasonably can be used. This section would prohibit employers, educational institutions, and others from using sensitive personal identification numbers or social security numbers for any employee benefit plan, card, or tag that is provided by employers, educational institutions, etc., for the purpose of identification. This section also would prohibit the use of social security numbers as driver identifiers on state drivers' licenses.

Section 8(c) would amend the Social Security Act (42 U.S.C. 405(c)(2)(C)) to prohibit any Federal, State, or judicial agency from employing or entering into a contract to use prison inmates that would allow access to the social security account numbers of other individuals. This prohibition would go into effect 90 days after the date of enactment.

Section 9. Information Security Working Group.

Section 9 would require the Chairman of the FTC to establish an Information Working Group, comprised of industry participants, consumer groups, and other interested parties to develop best practices to protect sensitive personal information. The Working Group would be required to submit to Congress a report on its findings within 12 months after its establishment.

Section 10. Definitions.

Section 10 would provide for a number of notable definitions, as follows:

Breach of Security: The unauthorized access to and acquisition of data in any form or format containing sensitive personal information that compromises the security or confidentiality of such information and establishes a basis to conclude that a reasonable risk of identity theft to an individual exists.

Consumer Reporting Agency: Any person which engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing credit reports to third parties.

Covered Entity: A sole proprietorship, partnership, corporation, trust, estate, cooperative, sole propriety, association, or other commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes sensitive personal information.

Credit Report: A consumer report as defined in section 603(d) of the Federal Fair Credit Reporting Act (15 U.S.C. 1681a(p)), that is used for the purpose of serving as a factor in establishing a consumer's eligibility for credit for personal, family or household purposes.

Identity Theft: The unauthorized acquisition, purchase, sale, or use by any person of an individual's sensitive personal information that violates section 1028 of title 18, USC, or any provision of State law; or results in economic loss to the individual whose sensitive personal information was used.

Reviewing the Account: Includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

Sensitive Personal Information: An individual's name, address, or phone number linked to one or more defined identifying data elements and any other identifying information determined by the FTC through a rulemaking process.

Public Records: Nothing in the Act would prohibit a covered entity from obtaining, aggregating, or using sensitive personal information it lawfully obtains from public records in a manner that would not violate this Act.

Section 11. Authorization of Appropriations.

Section 11 would authorize $1,000,000 to the FTC to carry out this Act for fiscal years 2006 through 2010.

Section 12. Effective Date.

Under this Act, the FTC would be required to initiate rulemakings under sections 2, 3, and 4 of this Act within 45 days after enactment and promulgate final rules within 1 year after the date of enactment of this Act. The requirements under sections 2, 3, and 4 determined by the FTC rulemaking would take effect 6 months after the final rule is promulgated.

All other provisions of this Act would take effect upon its enactment.

○