

2006 LEGISLATIVE PRIVACY & SECURITY RADAR

The Identity Theft Protection Act:

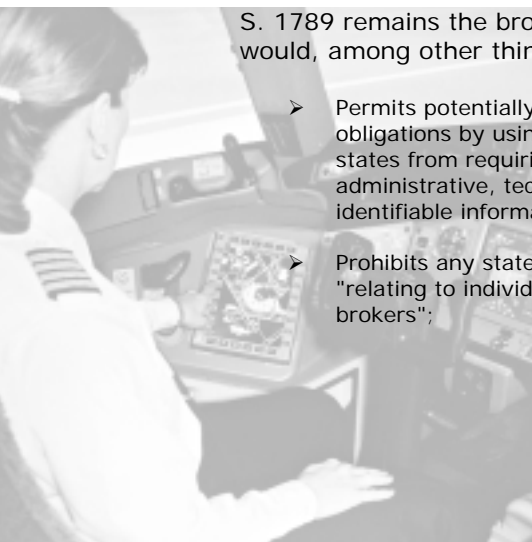
S. 1408 would generally create an affirmative obligation on all businesses nationwide to provide reasonable security for personal information over which they are custodians and to notify consumers of breaches in security that may pose a reasonable risk of identity theft. The bill would also create other obligations regarding security freezes and Social Security numbers:

- Preempt state laws requiring financial entities to maintain information security programs, notify individuals of security breaches regarding sensitive personal information, require security freezes, and prohibit the solicitation or display of Social Security numbers;
- Requires that any sensitive personal information that a covered entity sells, maintains, collects, transfers, or disposes of, in any form or format including paper, be full compliance with the FTC's existing rules on "Standards of Safeguarding Customer Information and Disposal of Consumer Report Information and Records" would be deemed compliance with this requirement);
- Require notification to consumers, the FTC, the functional regulators of certain industries (i.e., banking, insurance, etc.), and all consumer reporting agencies if more than 1,000 consumers are affected) whenever a "reasonable risk of identity theft" exists (as defined in the bill) following the discovery of a breach of security;
- Define "reasonable risk of identity theft" to mean that the "preponderance of the evidence available to the covered entity...establishes that identity theft for 1 or more individuals from the breach of security is foreseeable;"
- Define "sensitive personal information" as an individual's name, address, or telephone number, combined with one or more of the following data elements related to that individual: (1) Social Security number, taxpayer identification number, or "an employer identification number that is the same or is derived from the Social Security number of that individual," (2) financial account number, or credit card or debit card number (together with any required security code, access code, or password that would permit access to such individual's account), and (3) state driver's license identification number or state resident identification number;
- Empower the FTC to conduct a rulemaking to "designate other identifying information" as sensitive personal information for purposes of the act;
- Create a safe harbor for compliance with the bill's data security and notification provisions for those financial entities already obligated under, and in compliance with, title V of the Gramm-Leach-Bliley Act (GLBA) and section 607(a) of the Fair Credit Reporting Act (FCRA);
- Requires private financial entities to institute "security freezes" on consumer report information upon the demand of a consumer, regardless of whether such consumer is a victim of, or is at risk of falling victim to, identity theft;
- Prohibits the solicitation, purchase, sale, and display of Social Security numbers (with few exceptions); and authorize the FTC, functional regulators and state attorneys general to enforce the provisions of the act, but prohibit enforcement by private rights of action or class action lawsuits.

The Personal Data Privacy and Security Act of 2005:

S. 1789 remains the broadest form of federal data security legislation considered to date and would, among other things:

- Permits potentially inconsistent and/or conflicting state laws regarding data privacy and security obligations by using unclear and atypical legislative preemption language that only prohibits states from requiring covered financial entities to comply with "any requirements with respect to administrative, technical, and physical safeguards" for the protection of sensitive personally identifiable information;
- Prohibits any state law from imposing requirements or prohibitions regarding any subject matter "relating to individual access to, and correction of, personal electronic records held by data brokers";



- Preempt only any other provision of federal or state law "relating to" notification of a security breach (except that a state may require information regarding victim assistance and there is a carve-out for section 507 of GLBA);
- Requires, subject to limited safe harbors for financial and healthcare entities currently in compliance with federal data security regulations, that businesses collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. citizens must provide a data privacy and security program for protecting sensitive personally identifiable information;
- Requires, subject to certain exemptions, notification of security breaches upon the discovery of a "compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personal information that is unauthorized or in excess of authorization";
- Creates enhanced criminal penalties for identity theft and other violations of the bill, including a felony punishable by fine and up to 5 years in jail for any person who "intentionally and willfully conceals the fact" of a security breach;
- Establishes that consumer breach notification are to be provided red envelope whereby alerting the consumer of its importance;
- Defines "sensitive personally identifiable information" as either: (1) a financial account number or credit or debit card number, along with any required security code, access code, or password; or (2) an individual's first and last name or first initial and last name, in combination with any one of the following:
 1. Non-truncated Social Security number, driver's license number, passport number, or alien registration number;
 2. Any two of the following: (a) home address or telephone number; (b) mother's maiden name, "if identified as such"; or (c) month, day, and year of birth;
 3. Unique biometric data such as a fingerprint, voiceprint, retina or iris image, or "any other unique physical representation";
 4. A unique account identifier, electronic identification number, user name, or routing code along with any required associated security or access code, or password;
 5. Provides individuals an opportunity to review information maintained by data brokers and permit individuals to correct inaccuracies in that information;
 6. Provides for an exemption from breach notification requirements in the event a business entity determines, after a risk assessment, that there is no significant risk that the breach will result in harm to the individuals - the business entity must notify the U.S. Secret Service (USSS) of this finding, and the USSS must not object in writing to that conclusion within 10 days for the exemption to apply; and provide a cap of \$250,000 for each violation of data broker access/correction provisions, a cap of \$500,000 for each violation of data security obligations, and a cap on aggregate penalties for violations of breach notification requirements of \$50,000 per day.

Notification of Risk to Personal Data Act:

S. 1326, if enacted in would require covered financial entities nationwide to implement and maintain reasonable security and notification procedures and practices appropriate to the size and nature of the entity and the nature of the information it maintains:

- Preempts all state laws that relate in any way to electronic information security standards or security breach notification;
- Ties consumer notification requirements to circumstances when a "significant risk of identity theft" exists as a result of a security breach;

- Requires that "computerized" data containing sensitive personal information be protected from unauthorized access, destruction, use, modification or disclosure;
- Defines sensitive personal information in a manner nearly identical to the California definition—specifically, as a first and last name, and address or telephone number, in combination with one or more of the following data elements: a Social Security number, driver's license number, state identification number, financial account number, or credit or debit card number (in combination with any required security code, access code or password);
- Exempts from coverage encrypted data, truncated data, or otherwise publicly available information from the definition of sensitive personal information.

Data Accountability and Trust Act or "DATA":

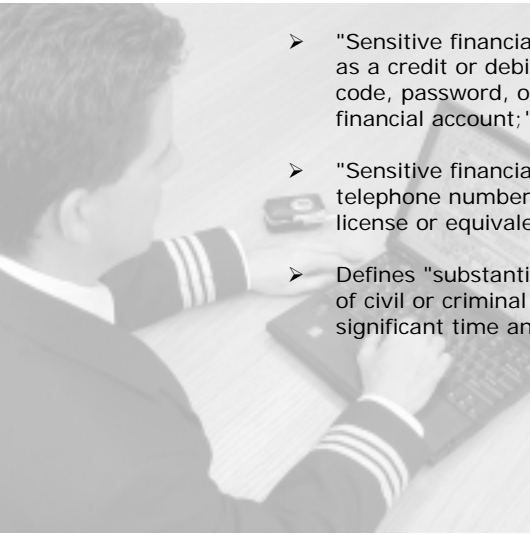
Requires financial entities to develop and implement security policies and procedures for the protection of personal information ("information brokers" would be required to submit their security policies to the FTC at the time of a breach notification or upon request by the FTC so that the FTC may conduct or require a post-breach audit of such policies);

- Requires notification of a breach of security where "the unauthorized acquisition of data in electronic form establishes a reasonable basis to conclude that there is a significant risk" to an individual, to whom the personal information relates, of being a victim of identify theft, fraud, or other unlawful conduct;
- Defines "personal information" as an individual's first name or initial and last name, or address, or phone number, in combination with any one or more of the following data elements: Social Security number, driver's license number, or other state identification number, or financial account number, credit or debit card number and any required security code, access code or password necessary to permit access to an individual's financial account;
- Requires financial entities notifying consumers of security breaches to provide, at no cost to each notified individual, quarterly consumer credit reports beginning no later than two months following discovery of a breach and continuing for a period of two years;
- Authorizes the FTC to enforce the act and conduct rulemakings to promulgate regulations regarding security policies and notification requirements, and to modify the definition of "personal information" (the act would also prohibit any person other than a state attorney general from bringing a civil action under state law if premised upon the defendant violating any provision of the act); and "supersede" state laws "expressly" affecting financial entities covered by H.R. 4127 until the act sunsets (unless reauthorized) 10 years after its date of enactment.

The Financial Data Protection Act of 2005:

Creates a new section 630 of the FCRA that would subject consumer reporting agencies, financial institutions and other businesses "assembling or evaluating" consumer reports, credit information or other information on consumers for various purposes, to new affirmative obligations to implement and maintain reasonable policies and procedures to protect the security and information of sensitive financial information of consumers "against any unauthorized use that is reasonably likely to result in substantial harm or inconvenience" to such consumers, and to notify them in the event of a breach of that security, defines "sensitive financial personal information" to include two kinds of information, as follows:

- "Sensitive financial account information," meaning a consumer's financial account number, such as a credit or debit card number, in combination with any security code, access code, biometric code, password, or other personal identification information that would allow access to the financial account;"
- "Sensitive financial identity information," meaning a consumer's first and last name, address, or telephone number, in combination with any of the following - social security number, driver's license or equivalent state identification number, or taxpayer identification number;
- Defines "substantial harm or inconvenience" as the "material financial loss" to, or the imposition of civil or criminal penalties upon, a consumer, or "the need for the consumer to expend significant time and effort to correct erroneous information relating to the consumer, including



information maintained by consumer reporting agencies, financial institutions, or government financial entities, in order to avoid material financial loss or increased costs or civil or criminal penalties, due to unauthorized use of sensitive financial personal information relating to such consumer";

- Requires financial entities notifying consumers of security breaches to offer a nationwide credit monitoring service to each consumer free of charge and for at least a 6-month period (so long as such service is requested by a consumer within 90 days of being notified of the security breach);
- Creates safe harbors for financial entities covered by, and in compliance with, title V of GLBA; and prohibits the imposition of state law requirements or prohibitions on financial entities covered by H.R. 3997 "with respect to the responsibilities' such financial entities to comply with the obligations under the act.

State Trends:

Starting with the passage of California's security breach notification legislation in 2002, twenty-two other states have adopted their own legislation on that original theme. Actions taken in 2005 by the various state legislatures varied widely, but certain general trends emerged creating a broader definition of personal information than California law, and include notification requirements for medical information, unique biometric data, electronic signatures, or account numbers regardless of whether they are accompanied by a required password.

Additionally, some state legislation requires notification of security breaches to be made to those other than affected consumers, including consumer reporting agencies and state regulatory authorities. With two exceptions (California and New York), state legislation generally does not preempt local government data security laws or ordinances. As a result, major metropolitan areas and localities (other than in California and New York) are free to pass more restrictive laws or ordinances.

Several states (and at least one municipality) are increasingly using security breach legislation as a vehicle for instituting other data security and privacy measures, including restrictions on the solicitation, display, collection or use of Social Security numbers, and requirements that consumer-reporting agencies verify adverse information in consumer reports.

In Summary:

In order to ensure a pragmatic and effective national privacy and security landscape, laws will need to be narrowly targeted at data security and breach notification, and that they include the following four core features: (1) national uniformity; (2) technology-neutral security standards to better safeguard sensitive personal data from unauthorized access (excepting financial entities, including financial institutions, now covered under existing law); (3) a reasonable notification trigger, following a breach of security, by which business customers, and consumers generally, would be informed when their identities are exposed to a "significant risk" of identity theft or misuse; and (4) administrative enforcement by which experienced federal agencies, and state attorneys general, can exercise oversight and take action to punish those who fail to live up to their obligations to consumers.

Unfortunately, Congress favors broad-based legislation that would go well beyond addressing the security of data containing sensitive personal information. Among other proposals, some would redefine data security as a data "privacy" issue and impose European-style opt-in data handling policies on American industry, without a parallel adjustment in compliance and enforcement policies. Such legislation might also include broadened consumer rights to "access and correct" personal information pertaining to them that is held by a business, as well as requirements for businesses to obtain a consumer's voluntary, affirmative consent before using personal information, even if acquired from publicly available records, this would fundamentally change the landscape for financial institutions.

