SECTION-BY-SECTION ANALYSIS FOR THE
PERSONAL DATA PRIVACY AND SECURITY ACT OF 2011

FOR GUIDANCE PURPOSES ONLY

Section 1. Short Title

This section provides that the legislation may be cited as the "Personal Data Privacy and Security Act of 2011."

Title I – Enhancing Punishment for Identity Theft and Other Violations of Data Privacy and Security

Section 101 – Organized Criminal Activity in Connection with Unauthorized Access to Personally Identifiable Information

Section 101 amends 18 U.S.C. § 1961(1) to add intentionally accessing a computer without authorization to the definition of racketeering activity.

Section 102 - Concealment of Security Breaches Involving Personally Identifiable Information

Section 102 makes it a crime for a person who knows of a security breach requiring notice to individuals under Title III of this Act, and of the obligation to provide such notice, to intentionally and willfully conceal the fact of, or information related to, that security breach. Punishment is either a fine under Title 18, or imprisonment of up to 5 years, or both.

Section 103 – Penalties for Fraud and Related Activity in Connection with Computers

Section 103 amends title 18, United States Code, section 1030(c) to clarify that both conspiracy to commit a computer hacking offense and attempt to commit a computer hacking offense are subject to the same criminal penalties as the criminal penalties for substantive violations of section 1030(c).

Title II- Data Brokers

Title II addresses the data brokering industry that has come of age, prompted by technology developments and changes in marketplace incentives. Data brokers collect and sell billions of private and public records about individuals, including personal, financial, insurance, medical and "lifestyle" data, as well as other sensitive information, such as details on neighbors and relatives, or even digital photographs of individuals. Companies like ChoicePoint, LexisNexis and Acxiom, which are generally regarded as leaders in this industry, use this information to provide a variety of products and services, including fraud prevention, identity verification, background screening, risk assessments, individual digital dossiers and tools for analyzing data.

Although some of the products and services offered by data brokers are subject to existing privacy and security protections aimed at credit reporting agencies and the financial industry under the Fair Credit Reporting Act ("FCRA") and Gramm-Leach-Bliley ("GLB"), many are not subject to such protections. In addition, there has been insufficient oversight of the industry's practices, including the accuracy and handling of sensitive data. These concerns have been highlighted by numerous reports of harm caused by inaccurate data records. This Title draws from the principles in FCRA and GLB to close these loopholes.

Section 201 – Transparency and Accuracy of Data Collection

Section 201 applies disclosure and accuracy requirements to data brokers that engage in interstate commerce and offer any product or service to third parties that allows access to, or use, compilation, distribution, processing, analyzing or evaluating of personally identifiable information. Section 201 requirements are not applicable to products and services already subject to similar disclosure and accuracy provisions under FCRA and GLB, and implementing regulations.

Section 201 requires data brokers to disclose to individuals, upon their request and for a reasonable fee, all personal electronic records pertaining to that individual that the data broker maintains for disclosure to third parties. Section 201 also requires data brokers to establish a fair process for individuals to dispute, flag or correct inaccuracies in any information that was not obtained from a licensor or public record. Modeled after Section 611 of FCRA, Section 201 requires data brokers to: (1) investigate disputed information within 30 days; (2) notify any data furnishers who provided disputed information and identify such data furnishers to the individual disputing the information; (3) provide notice to individuals on dispute resolution procedures and the status of dispute investigations, including whether the dispute was determined to be frivolous or irrelevant, whether the disputed information was confirmed to be accurate, or whether the disputed information was deleted as inaccurate; and (4) allow individuals to include a statement of dispute in the electronic records containing the disputed personal information. If the information was obtained from a licensor or public record, the data broker must provide the individual with contact information for the source of the data.

Section 201 also provides that, under circumstances where a person or business takes an adverse action regarding a consumer, which is based in whole or in part on data maintained by a data broker, the person or business must notify the consumer in writing of the adverse action and provide contact information for the data broker that furnished the information, a copy of the information at no cost and the procedures for correcting such information. There is an exemption for fraud databases.

Section 202 – Enforcement

A data broker that violates the access and correction provisions of Section 201 is subject to penalties of $1,000 per violation per day with a maximum penalty of $250,000 per violation. A data broker that intentionally or willfully violates these provisions is subject to additional penalties of $1,000 per violation per day, with a maximum of an additional penalty of $250,000 per violation.

The Federal Trade Commission ("FTC") will enforce Section 202 and may bring an enforcement action to recover penalties under this provision. States have the right to bring civil actions under this Section on behalf of their residents in U.S. district courts, and this section requires that States provide advance notice of such court proceedings to the FTC, where practicable. The FTC also has the right to stay any state action brought under this Section and to intervene in a state action.

Section 203 – Relation to State Laws

Section 203 preempts State laws with respect to the access and correction of personal electronic records held by data brokers.

Section 204 – Effective Date

Section 204 provides that Title II will take effect 180 days after the date of the enactment of the *Personal Data Privacy and Security Act*.

Title III– Privacy and Security of Personally Identifiable Information

Subtitle A – A Data Privacy and Security Program

Section 301 – Purpose and Applicability of Data Privacy and Security Program

Section 301 addresses the data privacy and security requirements of Section 302 for business entities that compile, access, use, process, license, distribute, analyze or evaluate personally identifiable information in electronic or digital form on 10,000 or more U.S. persons. Section 301 exempts from the data privacy and security requirements of Section 302 businesses already subject to, and complying with, similar data privacy and security requirements under GLB and implementing regulations, as well as examination for compliance by Federal functional regulators as defined in GLB, and HIPPA regulated entities.

Section 302 – Requirements for a Data Privacy and Security Program

Section 302 requires covered business entities to create a data privacy and security program to protect and secure sensitive data. The requirements for the data security program are modeled after those established by the Office of the Comptroller of the Currency for financial institutions in its *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 12 C.F.R. § 30.6 Appendix B (2005).

A data privacy and security program must be designed to ensure security and confidentiality of personal records, protect against anticipated threats and hazards to the security and integrity of personal electronic records, protect against unauthorized access and use of personal records, and ensure proper back-up storage and disposal of personally identifiable information. In addition, Section 302 requires a covered business entity to: (1) regularly assess, manage and control risks to improve its data privacy and security program; (2) provide employee training to implement its data privacy and security program; (3) conduct tests to identify system vulnerabilities; (4) ensure that overseas service providers retained to handle personally identifiable information, but which are not covered by the provisions of this Act, take reasonable steps to secure that data; and (5) periodically assess its data privacy and security program to ensure that the program addresses current threats. Section 302 also requires that the data security program include measures that allow the data broker (1) to track who has access to sensitive personally identifiable information maintained by the data broker and (2) to ensure that third parties or customers who are authorized to access this information have a valid legal reason for accessing or acquiring the information.

Section 303 - Enforcement

Section 303 gives the FTC the right to bring an enforcement action for violations of Sections 301 and 302 in Subtitle A. Business entities that violate sections 301 and 302 are subject to a civil penalty of not more than $5,000 per violation, per day and a maximum penalty of $500,000 per violation. Intentional and willful violations of these sections are subject to an additional civil penalty of $5,000 per violation, per day and an additional maximum penalty of $500,000 per violation. This section also grants States the right to bring civil actions on behalf of their residents in U.S. district courts, and requires States to give advance notice of such court proceedings to the FTC, where practicable. There is no private right of action under this subtitle.

Section 304 – Relation to Other Laws

Section 304 preempts state laws relating to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information. The requirements referred to in this Section are the same requirements set forth in Section 302.

Subtitle B – Security Breach Notification

Section 311 – Notice to Individuals

Section 311 requires that a business entity or federal agency give notice to an individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, compromised, following the discovery of a data security breach. The notice required under Section 311 must be made without unreasonable delay. Section 311(b) requires that a business entity or federal agency that does not own or license the information compromised as a result of a data security breach notify the owner or licensee of the data. The owner or licensee of the data would then provide the notice to individuals as required under this Section. However, agreements between owners, licensees and third parties regarding the obligation to provide notice under Section 311 are preserved.

Section 312 – Exemptions

Section 312 allows a business entity or federal agency to delay notification by providing a written certification to the U.S. Secret Service that providing such notice would impede a criminal investigation, or damage national security. This provision further requires that the Secret Service must review all certifications from business entities (and may review certifications from agencies) seeking an exemption from the notice requirements based upon national security or law enforcement, to determine if the exemption sought has merit. The Secret Service has 10 business days to conduct this review, which can be extended by the Secret Service if additional information is needed. Upon completion of the review, the Secret Service must provide written notice of its determination to the agency or business entity that provided the certification. If the Secret Service determines that the exemption is without merit, the exemption will not apply. Section 312 also prohibits federal agencies from providing a written certification to delay notice, to conceal violations of law, prevent embarrassment or restrain competition.

Section 312(b) exempts a business entity or agency that conducts a risk assessment after a data breach occurs, and finds no significant risk of harm to the individuals whose sensitive personally identifiable information has been compromised, from the notice requirements of Section 311, provided that: (1) the business entity or federal agency notifies the Secret Service of the results of the risk assessment within 45 days of the security breach and (2) the Secret Service does not determine within 10 business days of receipt the notification that a significant risk of harm does in fact exist and that notice of the breach should be given. Under Section 312(b) a rebuttable presumption exists that the use of encryption technology, or other technologies that render the sensitive personally identifiable information indecipherable, and thus, that there is no significant risk of harm.

Section 312(c) also provides a financial fraud prevention exemption from the notice requirement, if a business entity has a program to block the fraudulent use of information -- such as credit card numbers -- to avoid fraudulent transactions. Debit cards and other financial instruments are not covered by this exemption.

Section 313- Methods of Notice

Section 313 provides that notice to individuals may be given in writing to the individuals last known address, by telephone or *via* email notice, if the individual has consented to email notice. Media notice is also required if the number of residents in a particular state whose information was, or is reasonably believed to have been compromised exceeds 5,000 individuals.

Section 314 – Content of Notification

Section 314 requires that the notice detail the nature of the personally identifiable information that has been compromised by the data security beach, a toll free number to contact the business entity or federal agency that suffered the breach, and the toll free numbers and addresses of major credit reporting agencies. Section 314 also preserves the right of States to require that additional information about victim protection assistance be included in the notice.

Section 315 - Coordination of Notification with Credit Reporting Agencies

Section 315 requires that, for situations where notice of a data security breach is required for 5,000 or more individuals, a business entity or federal agency must also provide advance notice of the breach to consumer reporting agencies.

Section 316 – Notice to Law Enforcement

Section 316 requires that business entities and federal agencies notify the Secret Service of the fact that a security breach occurred within 14 days of the breach, if the data security breach involves: (1) more than 10,000 individuals; (2) a database that contains information about more than 1 million individuals; (3) a federal government databases; or (4) individuals known to be government employees or contractors involved in national security or law enforcement. The Secret Service is responsible for notifying other federal law enforcement agencies, including the FBI, and the relevant State Attorneys General within 14 days of receiving notice of a data security breach.

Section 317 - Enforcement

Section 317 allows the Attorney General to bring a civil action to recover penalties for violations of the notification requirements in Subtitle B. Violators are subject to a civil penalty of up to $1,000 per day, per individual and a maximum penalty of $1 million per violation, unless the violation is willful or intentional.

Section 318 – Enforcement by State Attorneys General

Section 318 allows State Attorneys General to bring a civil action in U.S. district court to enforce Subtitle B. The Attorney General may stay, or intervene in, any state action brought under this subtitle.

Section 319- Effect on Federal and State Law

Section 319 preempts state laws on breach notification, with the exception of state laws regarding providing consumers with information about victim protection assistance that is available to consumers in a particular State. Because the breach notification requirements in the bill do not apply to state and local government entities, this provision does not to preempt state or local laws regarding the obligations of state and local government entities to provide notice of a data security breach.

Section 320 – Authorization of Appropriations

Section 320 authorizes funds for the Secret Service as may be necessary to carry out investigations and risk assessments of security breaches under the requirements of Subtitle B.

Section 321 – Reporting on Risk Assessment Exemptions

Section 321 requires that the Secret Service report to Congress on the number and nature of data security breach notices invoking the risk assessment exemption and the number and nature of data security breaches subject to the national security and law enforcement exemptions.

Section 322 – Effective Date

Subtitle B takes effect 90 days after the date of enactment of the *Personal Data Privacy and Security Act.*

Title IV – Government Access to and Use of Commercial Data

Section 401 – General Services Administration Review of Government Contracts

Section 401 requires the General Services Administration (GSA), when issuing contracts for more than $500,000, to review and consider government contractors' programs for securing the privacy and security of personally identifiable information, contractors' compliance with such programs, and any data security breaches of contractors' systems and the responses to those breaches.

In addition, GSA is required to include penalties in contracts involving personally identifiable information for (1) failure to comply with Subtitle A (Data Privacy and Security Programs) and Subtitle B (Security Breach Notification) of Title III of this Act and (2) knowingly providing inaccurate information. Section 401 also requires that GSA include a contract requirement that government contractors exercise due diligence in selecting service providers that handle personally identifiable information and that government contractors take reasonable steps to select service providers that maintain appropriate data privacy and security safeguards.

Section 402 – Requirement to Audit Information Security Practices of Contractors and Third Party Business Entities

Section 402 amends 44 U.S.C. § 3544 to require that federal agencies audit and evaluate the information security practices of government contractors and third parties that support the information technology systems of government agencies.

Section 403 – Privacy Impact Assessment of Government Use of Commercial Information Services Containing Personally Identifiable Information

Section 403(a) updates the *E-Government Act of 2002* to require federal departments and agencies that purchase or subscribe to personally identifiable information from a commercial entity, to conduct privacy impact assessments on the use of those services. In addition, Section 403(b) requires federal departments and agencies that use such services to publish a description of the database, the name of the provider and the contract amount.

Section 403 also requires that federal departments and agencies adopt regulations that specify the personnel allowed to access government databases containing personally identifiable information and the standards for ensuring, among other things, the legitimate government use of such information, the retention and disclosure of such information, and the accuracy, relevance, completeness and timeliness of such information. Section 403 further provides that federal departments and agencies must include in contracts for more than $500,000 and agreements with commercial data services, penalty provisions for circumstances where a data broker delivers personally identifiable information that it knows to be inaccurate, or has been informed is inaccurate and is in fact inaccurate. Section 403(c) also requires that data brokers that engage service providers, who are not subject to the data security program requirements of the bill, exercise due diligence in retaining these service providers to ensure that adequate safeguards for personally identifiable information are in place.

Section 403(d) directs the Government Accountability Office to conduct a follow-up study and report to Congress on federal agency use of commercial databases, including the impact of such use on privacy and security, sufficiency of privacy and security protections, and the extent to which commercial data providers are penalized for privacy and security failures.

Title V – Compliance with Statutory Pay-As-You-Go Act

Section 501 - Budget Compliance

Section 501 contains the language required to comply with the Pay-As-You-Go Act.