

# The Data Security Act

---

INTRODUCED BY CONGRESSMAN RANDY NEUGEBAUER (R-TX) AND CONGRESSMAN JOHN CARNEY (D-DE)

## SECTION-BY-SECTION ANALYSIS

### Section 1: Short Title

- The “Data Security Act of 2015”

### Section 2: Purposes

- The purposes of this Act are to establish strong and uniform national data security and breach notification standards for electronic data, and to expressly preempt any related state laws in order to provide the Federal Trade Commission with authority to enforce such standards for entities covered under this Act.

### Section 3: Definitions

This section sets forth a number of definitions, including:

- “Covered Entity” – any individual, partnership, corporation, trust, estate, cooperative, association, or entity that accesses, maintains, communicates, or handles sensitive account information or sensitive personal information.
- “Breach of Data Security” – the unauthorized acquisition of sensitive financial account information or sensitive personal information. This does not include the unauthorized acquisition of sensitive financial account information or sensitive information that is encrypted, redacted, etc.
- “Information Security Program” – the safeguards that a covered entity uses to access, collect, distribute, process, protect, use transmit, dispose of, or otherwise handle sensitive financial account information and sensitive personal information.
- “Sensitive Financial Account Information” – a financial account number relating to a consumer, including a credit card number or debit card number in combination with any security code, access code, password, or other personal identification information required to access the financial account.
- “Sensitive Personal Information” – the social security account number or the first and last name of a consumer in combination with any of the following relating to the consumers:
  - Driver’s license number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
  - Information that could be used to access an individual’s account, such as a user name and password or email and password; or
  - Biometric data used to gain access to financial accounts.
- “Substantial Harm” – identity theft or fraudulent transactions on financial accounts.

# The Data Security Act

---

## **Section 4: Protection of Information and Security Breach Notification**

This section of the bill has three prominent subsections to address (a) data security, (b) investigation of potential breaches, and (c) breach notification.

### (a) Security Procedures Required

Each covered entity shall develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are reasonably designed to achieve the following objectives:

- Ensure the security and confidentiality of sensitive financial account and sensitive personal information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized acquisition of such information that could result in substantial harm.

Limitation: a covered entity's information security program shall be appropriate to:

- Size and complexity of the covered entity;
- Nature and scope of the activities of the covered entity; and
- Sensitivity of the consumer information to be protected.

Elements: In order to develop, implement, and maintain its information security program, a covered entity shall:

- Designate an employee or employees to coordinate the information security program;
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive account information and sensitive personal information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement information safeguards to control the risks identified in its risk assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.
- Oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the sensitive account information and sensitive personal information at issue; and to require service providers by contract to implement and maintain such safeguards by reasonably overseeing or obtaining an assessment of the service provider's compliance with contractual obligation where appropriate in light of the covered entity's risk assessment.
- Evaluate and adjust the information security program in light of the results of the risk assessments and testing and monitoring, and any material changes to the covered entity's operations or business arrangements, or any other circumstances that the covered entity knows may have a material impact on its information security program.

Security Controls: Each entity shall consider whether the following security measures are appropriate:

- Access controls on information systems;
- Access restrictions at physical locations;
- Encryption;
- Procedures to ensure information system modifications are consistent with its information security program;

# The Data Security Act

---

- Dual control procedures, segregation of duties, and employee background checks;
- Monitoring systems and procedures to detect actual or attempted attacks;
- Response programs that specify actions when unauthorized individuals have gained access to information systems; and
- Measures to protect against destruction, loss, or damage of sensitive account information or sensitive personal information due to environmental hazards.

Administrative Requirements: If a covered entity has a board of directors, the covered entity's board of directors or an appropriate committee of the board shall:

- Approve the information security program; and
- Oversee the development, implementation, and maintenance of the information security program.
- Receive, at least annually, a report describing the overall status of the information security program, its compliance with this Act, and recommendations for changes to the information security program.

## (b) Investigation Required

If a covered entity believes that a breach of data security has or may have occurred involving sensitive financial account information or sensitive personal information, the covered entity shall conduct an investigation to:

- Assess the nature and scope of the incident;
- Identify any sensitive account information or sensitive personal information that may have been involved;
- Determine if the sensitive account information or sensitive personal information has been acquired without authorization; and
- Take reasonable measures to restore the security and confidentiality of the systems compromised in the breach.

## (c) Notice Required

If a covered entity determines that the unauthorized acquisition of sensitive financial account information or sensitive personal information involved in a breach of data security is reasonably likely to cause substantial harm to the consumers to whom the information relates, the covered entity, or a third party acting on behalf of the covered entity shall notify without unreasonable delay:

- An appropriate federal law enforcement agency;
- An appropriate regulatory agency;
- Any relevant payment card network if the breach involves payment card numbers;
- Each consumer reporting agency if the breach involves sensitive personal information relating to 5,000 or more consumers; and
- All consumers to whom the sensitive account information or sensitive personal information relates.

Each covered entity shall provide notice to consumers by:

- Written notice sent to the postal address of the consumer (if on record);
- Telephone notice to the phone number of the consumer (if on record);
- Email notice or other electronic means (if on record);
- Substitute notification in print and to broadcast media if providing written, telephonic, or electronic notice is not feasible due to:

# The Data Security Act

---

- Lack of sufficient contact information for the consumer to be notified;
- Excessive cost to the covered entity; or
- Exigent circumstances.

Each covered entity shall provide notice that includes:

- A description of the type of sensitive account information or sensitive personal information involved in the breach of data security;
- A general description of the actions taken by the covered entity to restore the security and confidentiality of the sensitive account information or sensitive personal information involved in the breach;
- A summary of rights of victims of identity theft prepared by the Federal Trade Commission under the Fair Credit Reporting Act if the breach involved sensitive personal information.

Delay of notice permitted when requested by law enforcement:

- A covered entity can delay any notification when requested by law enforcement

## (d) Clarification

A financial institution shall have no obligation under this Act for a breach of security at another covered entity involving sensitive account information relating to an account owned by the financial institution.

## (e) Special Notification Requirements

**Third-party Service Providers** – In the event of a breach of data security of a system maintained by a third-party entity that has been contracted to maintain, store, or process data in electronic form containing sensitive account information or sensitive personal information on behalf of a covered entity who owns or possesses such data, such third party shall:

- Notify the covered entity; and
- Notify consumers if it is agreed in writing that the third-party service provider will provide such notification on behalf of the covered entity.

**Carrier Obligations** – if a telecommunications provider becomes aware of a breach of data security involving sensitive account or sensitive personal information that is owned or possessed by a covered entity that connects to or uses a system or network provided by the carrier for the purposes of transmitting or routing such data, the carrier shall notify the covered entity if they can be reasonably identified.

If a covered entity that is not a financial institution experiences a breach of data security involving sensitive account information, a financial institution that issues an account to which the sensitive account information relates may communicate with the account holder regarding the breach, including:

- An explanation that the financial institution was not breached, and that the breach occurred at a third-party that had access to the consumer's sensitive account information; or
- Identify the covered entity that experienced the breach after the covered entity has provided notice consistent with this Act.

## (f) Compliance

# The Data Security Act

---

Entities already in compliance with the requirements under Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, or the Health Information Technology for Economic and Clinical Health Act are deemed in compliance with this Act.

## **Section 5: Administrative Enforcement**

This section describes which relevant regulatory agency will have exclusive enforcement authority under the bill. For example, in the case of national banks and saving associations, the Office of the Comptroller of the Currency will be the responsible regulatory agency; whereas, in the case of state insurance companies, the appropriate state insurance authority will be responsible.

The Federal Trade Commission would be the responsible regulatory agency for any covered entity that is not subject to the jurisdiction of any agency or authority described in this section. It also preempts Federal Communications Commission enforcement authority over security and breach notification so the telecommunications sector has one regulator and one set of rules.

The section also provides that the act should not be construed to provide a private right of action, including a class action.

## **Section 6: Relation to State Law**

This section replaces and preempts the current patchwork of state safeguards and breach laws that adds confusion and costs to entities that operate across state lines and consumers affected by a breach.

## **Section 7: Delayed Effective Date**

Provisions of the Act take effect 1 year from date of enactment.