Summary of H.R. 2577
"The SAFE Data Act"

(July 20,2011)

H.R. 2577 was introduced on July 19. On July 20, the House Commerce Subcommittee on Commerce, Manufacturing and Trade approved the legislation moving it onto the full Commerce Committee for consideration.

The bill requires that Entities/Individuals engaged in interstate commerce that own or possess personal information related to commercial activity, including third parties who have contracted with such persons. "Personal Information" means an individual's first name or initial and last name, address or phone number in combination with any one or more of the following: 1) Social Security number 2) driver's license, passport or government id number or 3) financial account number or credit or debit card number and any required safety code, access code or password necessary to permit access to an individual's financial account.

Covered individuals/entities would be required to comply with two key elements:

- Implement data security policies with specific baseline requirements
    - All required policies/practices will take into consideration the size of, and the nature, scope and complexity of the activities engaged in by the entity as well as the costs required to comply
    - An entity that must comply with the Gramm-Leach-Bliley Act is exempted from this requirement

- In the event of a breach of electronic data involving unlawful activity, comply with a uniform national data breach notification standard that would supersede the current patchwork of state data breach notification laws.
    - Notification to law enforcement is required to be made within 48 hours of discovery
    - If it is determined, based on assessment that the breach presents a "reasonable" risk of identity theft, fraud or unlawful conduct notification must be made to within 48 hours to the FTC and as promptly as possible to the affected individuals.
    - If breach notification is required to be made to more than 5000 individuals, then major credit reporting agencies must also be notified
    - Notification will include a toll-free phone number to contact the entity in inquire about breach security and notice that the individual is entitled to free consumer credit reports or credit monitoring for 2 years following the breach notification.
    - A "substitute" notification process is required for entities that own or possess electronic data containing personal information of fewer than 1000 individuals and direct notification is not feasible.
    - "Substitute" notification is comprised of 1) email notification, 2) a conspicuous notice on the website of the person/entity or 3) notification in print or broadcast media.
    - "Substitute" notification will include notice that affected individuals are entitled to receive free credit reports on a quarterly basis for a period of 2 years except when the only information that has been subject to the breach is first name/initial and last name or address, or phone number in combination with a credit or debit card and any required security code.

- FTC given ability to write regulations that determine criteria for determining if costs exceed benefits of notification—it may also determine the circumstance under which credit reports/credit monitoring shall be provided.

- Electronic data rendered unusable, unreadable or indecipherable to an unauthorized person bey encryption or other security technology shall be presumed to be subject to exemption.

- Violations of the legislation would constitute unfair or deceptive acts or practices enforceable under the FTC Act and may result in civil penalties. While State Attorneys General have the right to bring civil actions on behalf of their residents, there is no private right of action.