



Following is a Synopsis of the Seamless Peer 2 Peer White Paper on Regulatory Compliance for Security of Wireless Data Transmission. For access to the full report, please visit www.slwf.net

Peer2Peer Security and Compliance with Pending Specter-Leahy and Existing HIPAA, SOX, and DoD 8100.2 Regulations

Compliance with Regulatory Policies for Security of Wireless Data Transmission

In today's communications environment, organizations are challenged by the necessity to comply with the various regulations regarding data and personal information security. Vertical industries are subject to data security regulations germane to their operational spheres, such as medical information/HIPAA, public companies/Sarbanes-Oxley (SOX), and defense and homeland security/DoD 8100.2.

Security compliance is designed to prevent and mitigate identity theft, ensure privacy and provide notice of security breaches to affected individuals and enhance criminal penalties, law enforcement assistance and other protections against security breaches, fraudulent access and misuse of personally identifiable information.

Databases of personally identifiable information are increasingly prime targets of hackers, identity thieves and other criminals. Identity theft is a serious threat to the nation's economic stability, homeland security, e-commerce and American privacy rights.

The pending Specter-Leahy bill will require agencies and businesses to enact a comprehensive data privacy and security program, including technical safeguards such as encryption for protecting personally identifiable information during use, transmission, storage and disposal. Potential penalties for an organization for noncompliance are considerable, including a civil fine of \$5,000 per violation per day up to a daily maximum of \$35,000 and if an organization does not notify individuals of a security breach the bill proposes a civil fine of \$1,000 per day for every individual not notified in a timely way up to a daily maximum of \$50,000. The bill also stipulates that any person willfully or intentionally concealing a security breach can be imprisoned for up to 5 years.

Encryption as the Foundation for Compliance

Encryption is the simplest, most effective way to achieve compliance with data privacy and protection regulations. Most regulations, including Specter-Leahy, HIPAA, Sarbanes-Oxley, either recommend or require encryption as part of a data security program, and nearly every federal governing body (the SEC, FTC, FDA, NIST and so on) endorses encryption as an effective safeguard. In the wireless sphere organizations that use robust encryption schema will be able to effectively demonstrate their data privacy compliance to the various regulatory agencies.

By adopting the Seamless Phenom® wireless data security solution, organizations gain the ability to implement encryption-based security as a simple and small client download that that can be deployed using standard distribution methods and administrated alongside all other group policies. Enterprise organizations and their employees are then empowered to seamlessly and easily encrypt data on a consistent and constant basis.