NEW YORK ENACTS INFORMATION SECURITY BREACH AND NOTIFICATION ACT; ENTITIES THAT CONDUCT BUSINESS IN NEW YORK AND POSSESS COMPUTERIZED DATA MUST COMPLY BY DECEMBER 2005

In response to a recent wave of high-profile data security breaches, New York Governor George E. Pataki signed A.B. 4254, the Information Security Breach and Notification Act (the "Act") on August 9, 2005. The Act requires persons and companies that conduct business in New York State to notify state residents of acquisition by unauthorized parties of sensitive or "private" information. Entities that conduct business in New York State, especially those that do not currently encrypt data, should become familiar with the requirements of the new legislation, which takes effect on or about December 7, 2005.

1. The Information Security Breach and Notification Act

The Act requires entities that conduct business in New York State and own or license "private" data to notify state residents affected by any security breach that results in unauthorized acquisition of that data. "Private" data is defined as unencrypted computerized information that can identify the individual, combined with one of the following data elements: a) social security number, b) driver's license or non-driver identification card number or c) financial account information such as credit or debit card numbers in combination with access codes or PIN numbers. Private data is considered to be unencrypted when either the identifying information or the data element is not encrypted or is encrypted with a key that has also been acquired. Notification must be provided directly to the affected persons by a) written notice, b) electronic notice if the affected person has expressly consented to receiving the information in electronic form, c) telephone notice or d) under certain conditions, e-mail notice, conspicuous posting of the notice on the website of the affected business, and notification to major statewide media.

In addition, persons or businesses that maintain, but do not own, private data are obligated to notify the entity that owns or licenses the data when a security breach results in unauthorized access. Under the Act, the data owner or licensee most likely remains responsible for notifying the individuals affected by the security breach.

The Act further authorizes the New York State Attorney General to sue a business violating the statute in order to recover damages for actual costs or losses, including consequential financial losses incurred by persons entitled to notification. If a business engages in knowing or reckless violations, the court can impose a civil penalty of the greater of $5,000, or $10 per instance of failed notification up to $150,000. Moreover, the Act adds that "the remedies provided by this section shall be in addition to any other lawful remedy available," possibly permitting private actions.

The Act is applicable to every entity that conducts business in New York State and possesses data as seemingly innocuous as a computerized human resources database that includes employee social security numbers. The Act could also apply to many other financial and data service provider databases. A breach of security under the Act does not require a sophisticated computer network; while computer hackers circumvent network firewalls to cause security breaches, a lost or stolen laptop could also trigger the Act's notification requirements.

2. Actions of Other States and Congress

The Act follows in the wake of California's data protection law, as well as a growing number of other state laws. At least 35 states introduced similar legislation in the first seven months of 2005. At least 18 of those bills were signed into law in states including Connecticut, Delaware, Florida, Georgia, Illinois, Nevada and Rhode Island. The application of these state laws -- including the New York Act -- to financial institutions is not preempted by the federal Gramm-Leach-Bliley Disclosure of Nonpublic Personal Information Act, which permits states to impose standards of data security that are stricter than those enforced by the federal government.

Congress is also likely to strengthen federal data security laws, with several bills currently under serious consideration. Before adjourning for the August recess, the Senate Commerce Committee unanimously approved the Identity Theft Protection Act of 2005, introduced by Senators Gordon Smith (R-OR) and Bill Nelson (D-FL). The proposed legislation sets national standards to safeguard individual personal information, to notify consumers of data breaches and to require businesses to improve their safeguards for sensitive consumer information. The bill covers any entity that collects or otherwise acquires sensitive personal information, including social security numbers, financial account information, driver's license information and any other information that the Federal Trade Commission (the "FTC") determines can be used for identity theft. Entities that possess sensitive personal information would be required to secure it with physical and technological safeguards to be specified by the FTC. The legislation also authorizes fines of $11,000 per individual consumer affected by a security breach, up to $11 million per breach.

The Senate Judiciary Committee is also considering three personal data security bills, including the Personal Data Privacy and Security Act introduced by Senators Arlen Specter (R-PA) and Patrick Leahy (D-VT), which requires entities that maintain personal data to give notice to individuals and law enforcement agencies when they experience a breach involving sensitive personal data.

3. Data Security Practices

In light of these legislative developments, entities that conduct business in New York State must be particularly vigilant to ensure that private data is secure. At a minimum, a person or business that possesses private data should:

1. implement procedures to monitor and review databases and other computerized information storage devices to identify where private data is stored; and

2. establish clear and effective notification procedures to respond to actual breaches of security.

Other steps that suit the particular circumstances of a person or business that owns, licenses, maintains or otherwise possesses computerized private data can be tailored to help prevent security breaches and to satisfy the requirements of the Information Security Breach and Notification Act.

****

If you have any questions concerning the foregoing or would like further information, please call Stephen Bell at 202-303-1102, Sophie Keefer at 202-303-1142 or Karen Henein at 202-303-1255, located in our Washington, DC office, or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is 212-728-8000 and our facsimile number is 212-728-8111. Our website is located at www.willkie.com.

August 22, 2005

Copyright © 2005 by Willkie Farr & Gallagher LLP

All Rights Reserved. This memorandum may not be reproduced or disseminated in any form without the express permission of Willkie Farr & Gallagher LLP. This memorandum is provided for news and information purposes only and does not constitute legal advice or an invitation to an attorney-client relationship. While every effort has been made to ensure the accuracy of the information contained herein, Willkie Farr & Gallagher LLP does not guarantee such accuracy and cannot be held liable for any errors in or any reliance upon this information.