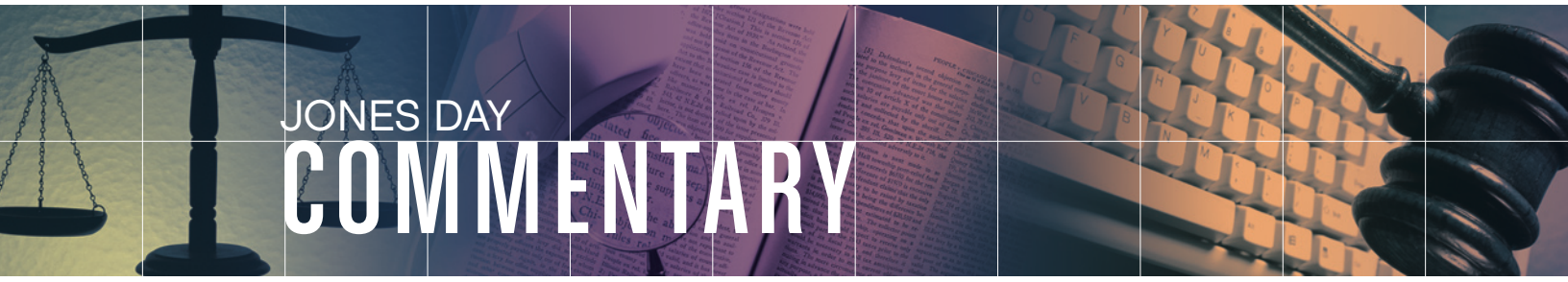
FEBRUARY 2006



DATA PROTECTION AND PRIVACY

OHIO ENACTS SECURITY BREACH NOTIFICATION LAW

Effective February 17, 2006, Ohio will join a growing list of states that require notification of individuals whose electronic personal information has been the subject of a security breach. The new security breach notification law (the "Notification Law") applies to Ohio governmental agencies and to individuals and entities that conduct business in Ohio (each a "Covered Entity"). Although the concept of "conducting business" is not clearly defined in the Notification Law, it appears that a physical presence in Ohio is not required. Thus, any entity that does business in Ohio and collects or maintains personal information will be a Covered Entity unless it is expressly exempted from the Notification Law. After the effective date of the Notification Law, a Covered Entity will be required to notify any Ohio resident whose personal information was acquired, or is reasonably believed to have been acquired, through a "breach of the security of a system" of a Covered Entity's computerized database. Certain financial institutions and health care entities are exempted from the Notification Law, but the vast majority of companies doing business in Ohio must adhere to these notice requirements. The requirements of the Notification Law cannot be waived by residents through contractual agreement or otherwise. This *Data Protection and Privacy Commentary* briefly summarizes the new Ohio law and provides strategies for improving security compliance efforts.

SECURITY BREACH NOTIFICATION STATUTE

The Notification Law requires each Covered Entity that owns or licenses computerized data to disclose certain breaches of the security of its system. For purposes of Ohio law, a "breach of the security of a system" requires the following elements: (i) an unauthorized person accesses and acquires computerized data of a Covered Entity (*i.e.*, information stored in an electronic medium), (ii) such access and acquisition compromises the security and confidentiality of the personal information owned or licensed by a Covered

Entity, and (iii) the access and acquisition of such personal information causes or is reasonably believed to have caused (or will cause) a material risk of identity theft or other fraud to an Ohio resident. If such a security breach occurs, the Covered Entity must notify each Ohio resident whose personal information was, or is reasonably believed to have been, accessed and acquired. Additionally, the Notification Law requires companies that maintain computerized data on behalf of other persons to expeditiously notify the owner of the computerized data of any security breach of a system containing the owner's data.

Under the Notification Law, "personal information" means an individual's first name or first initial and last name, in combination with one of the following data elements:

- A Social Security number.
- A driver's license number or state identification card number.
- An account number or credit/debit card number in combination with any required access code to that account or card.

The Notification Law is not triggered if these data elements are encrypted, redacted to four digits, or otherwise made to be unreadable. Further, personal information does not include information that is lawfully made available to the general public from government records or certain widely distributed media reports (*e.g.*, published in a bona fide newspaper, journal, or magazine or broadcast over radio or television).

NOTICE OBLIGATIONS UPON A BREACH OF SECURITY

Unless doing so would impede a criminal investigation or compromise homeland or national security, a Covered Entity must notify an Ohio resident whose personal information was subject to a breach of the security of a system in the most expedient time possible, but in no event later than 45 days after learning of the breach. A person or entity that holds computerized personal information on behalf of a Covered Entity must notify the Covered Entity expeditiously of any applicable security breach, but no specific time period for such notification is prescribed by the Notification Law.

The Notification Law does not specify the contents of the notification, but it would be advisable to have a consistent message prepared that describes the date of the breach, the information disclosed, the Covered Entity's actions in response to the breach, and a toll-free telephone number and e-mail address to which questions concerning the disclosure can be directed. The Covered Entity may inform the affected Ohio resident in writing or by telephone. Electronic notification is also acceptable, but only if the Covered Entity primarily communicates with the resident through electronic means. Although not required by the Notification Law, Covered Entities should also consider ways to remediate any potential harm that may be caused by the disclosure, such as paying for credit-monitoring services for individuals affected by the disclosure.

If the Covered Entity lacks sufficient contact information for the Ohio resident, or more than 500,000 persons must be notified, the Covered Entity may use an alternative notification method specified in the Notification Law, which involves e-mail notification, conspicuous disclosures on the Covered Entity's web site, and notification of the major media outlets. This alternative method is also available if the cost of making a disclosure exceeds $250,000. For Covered Entities with 10 or fewer employees, an alternative notification method (including ads in local newspapers, disclosures on the Covered Entity's web site, and media outlet notification) is available if disclosure costs exceed $10,000.

In addition to notifying Ohio residents, a Covered Entity may be required to notify consumer reporting agencies. If a single security breach of a system mandates notification to more than 1,000 Ohio residents, the Covered Entity must notify all nationwide consumer reporting agencies, without unreasonable delay, of the timing, distribution, and content of the disclosure given to the residents.

NOTABLE EXEMPTED ENTITIES

The Notification Law does not apply to certain financial institutions and health care entities that are subject to federal regulatory requirements involving the privacy and security of an individual's information. Specifically, a financial institution, trust company, or credit union (or any affiliate thereof) is

exempt from the requirements of the Notification Law if such entity is required by federal statute, regulation, or other regulatory action to notify its customers of an information security breach with respect to information about those customers and is subject to examination by its functional government regulatory agency for compliance with the applicable federal law. Further, the Notification Law does not apply to any person or entity that is regulated by sections 1171 to 1179 of the Social Security Act, chapter 531, 49 Stat. 620 (1935), 42 U.S.C. 1320d to 1320d-8, and any corresponding regulations in 45 C.F.R. Parts 160 and 164 (better known as the privacy and security regulations under the Health Insurance Portability and Accountability Act of 1996, or "HIPAA"). This means that the Notification Law does not apply to most health care providers, health plans, and health care clearinghouses.

CONSEQUENCES OF NONCOMPLIANCE

The Notification Law creates a strong incentive for Covered Entities to design and maintain procedures that will limit the vulnerability of their computer systems and that outline a course of action to pursue in the event of a security breach. Covered Entities that fail to secure their systems face the cost of notification and the negative impact on image and consumer confidence associated with publicly disclosing a security breach. If a Covered Entity fails to comply with the Notification Law's requirements, the Ohio attorney general may investigate and sue companies suspected of violating the statute, and courts may impose damages of up to $10,000 per day, depending on how long the Covered Entity fails to comply with the Notification Law.

STRATEGIES FOR SECURITY AND COMPLIANCE

Covered Entities should review their existing practices and systems for protecting the privacy and security of personal data. Covered Entities should also ensure that the requirements of the Notification Law are appropriately integrated into their security and privacy policies and procedures. Additionally, Covered Entities should consider implementing other measures to ensure compliance, such as:

- Determining what personal information is collected and maintained on computer systems and how it is stored.
- Utilizing effective technologies to identify and understand potential security gaps and to monitor systems and report detected security breaches.
- Encrypting or redacting to four digits identifying numbers (*e.g.*, Social Security numbers, driver's license numbers, state identification numbers, and account and credit card numbers).
- Training employees on the importance of information protection and immediate reporting of breaches.
- Determining the contact information for, and the best means of notifying, the affected individuals in the event of a security breach involving personal information.
- Developing internal assessment procedures and contingency plans for investigating the scope and source of a security breach, possibly with the assistance of outside investigators, and for taking corrective actions to remediate harm and prevent further breaches.
- Developing a contingency public relations plan to minimize damage to the Covered Entity's reputation resulting from a security breach.
- Reviewing representations made concerning security, privacy, and notification procedures.
- If a Covered Entity uses a third party to maintain its computerized database of personal information, reviewing and revising contracts with the third party to ensure compliance with notification and reporting obligations and to indemnify the Covered Entity for damages caused by the third party's breach of its obligations.

CONCLUSION

Ohio is following a national trend in passing a security breach notification statute. Companies that conduct business in Ohio are well advised to monitor this development and revise their security practices accordingly. The various state statutes provide a strong incentive for companies to develop comprehensive information security procedures that minimize the risk of, and address appropriate responses to, a security breach.

RELATED *JONES DAY COMMENTARIES*

- "New York Enacts Data Security and Notification Law" – August 2005
- "California Raises the Bar on Data Security and Privacy" – September 2003
- "Privacy Issues in Cross-Border Transactions" – June 2003

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. We invite you to visit our web site for additional information on privacy topics. General e-mail messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Jeffrey L. Kapp
1.614.281.3949
jlkapp@jonesday.com

Kevin D. Lyles
1.614.281.3821
kdlyles@jonesday.com

David W. Sloan
1.216.586.7233
dwsloan@jonesday.com

Rose Mary Wenstrup
1.216.586.7018
rwenstrup@jonesday.com