

SCHWARTZ & BALLEN LLP
1990 M STREET, N.W. • SUITE 500
WASHINGTON, DC 20036-3465
(202) 776-0700

FACSIMILE
(202) 776-0720

www.schwartzandballen.com

M E M O R A N D U M

September 22, 2005

To Our Clients and Friends

Re: State Security Breach Laws

This memorandum summarizes state legislation requiring notification to consumers of unauthorized disclosures of their personal information.¹ Twenty states have enacted legislation addressing security breaches. Most recently, Connecticut, Delaware, Florida, Illinois, Louisiana, Maine, Minnesota, Nevada, New Jersey, New York, North Carolina, Rhode Island, Texas and Tennessee have enacted legislation regarding this subject.

If you have any questions, please call Gilbert Schwartz, Robert Ballen or Tom Fox at (202) 776-0700.

ARKANSAS

Arkansas law (SB 1167) (Ark. Code Ann. §§ 4-110-101 et seq.) requires that a person that acquires, owns or licenses computerized data that includes personal information disclose a breach of the security of the system to any Arkansas resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice is not required if after reasonable investigation the person determines there is no reasonable likelihood of harm to customers. The law was effective August 12, 2005.

Written or electronic notice must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or

¹ The summaries presented below generally discuss the significant portions of the state laws.

SCHWARTZ & BALLEN LLP

electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media.

"Personal information" is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted or redacted:

- Social Security number;
- Driver's license or state identification card number;
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; or
- Medical information.

The act does not apply to persons regulated by state or federal law that provides "greater protection" to personal information and at least as thorough disclosure requirements for breaches of personal information as under Arkansas law.

A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

A violation of the act constitutes a Class A misdemeanor, punishable by up to one year in prison and a fine of up to \$1,000. The State Attorney General also is authorized to seek an injunction against any business in violation of the act.

CALIFORNIA

California law (Cal. Civ. Code §§ 1798.80 et seq.) requires a person conducting business in California that owns or licenses computerized data including personal information to disclose any breach of the security of the system to any resident of California whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. A "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person. The law was effective July 1, 2003.

SCHWARTZ & BALLEN LLP

Written or electronic notice must be given upon discovery or notification of the breach in the most expedient time possible and without unreasonable delay consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media.

"Personal information" is an individual's name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social Security number;
- Driver's license number or California identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

Any customer injured by a violation may institute a civil action to recover damages. Additionally, a person that violates the act may be enjoined from future violations.

CONNECTICUT

Connecticut law (SB 650) (Public Act 05-148) requires that a person conducting business in the state that owns, licenses or maintains computerized data that includes personal information disclose a breach of the security of the system to any Connecticut resident whose unencrypted personal information was or is reasonably believed to have been accessed by an unauthorized person. Notice is not required if after reasonable investigation and consultation with law enforcement the person determines there is no reasonable likelihood of harm to customers. The law is effective January 1, 2006.

SCHWARTZ & BALLEN LLP

Notice must be given without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach, identify the individuals affected and restore the reasonable integrity of the data system. Notice may be written, electronic or telephonic. As an alternative, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written, telephonic or electronic notice.

"Personal information" is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted or otherwise rendered unreadable or unusable:

- Social Security number;
- Driver's license or state identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

A person that maintains notification procedures (1) as part of an information security policy for the treatment of personal information, in which the notification is consistent with the timing requirements of the law or (2) pursuant to the rules, regulations, procedures or guidelines established by the person's primary or functional federal regulator, is deemed to be in compliance with the notification requirements of the law.

A violation of the act constitutes an unfair trade practice and is enforced by the State Attorney General. Any customer injured by a violation may institute a civil action to recover damages and may recover reasonable attorney's fees and costs. Additionally, any person that violates the act may be enjoined from future violations.

DELAWARE

Delaware law (HB 116) (Del. Code Ann. Tit. 6, §§ 12B-101 et seq.) requires that an individual conducting business in the state that owns or licenses computerized data that includes personal information about a Delaware resident conduct a reasonable and prompt investigation when it becomes aware of a breach of security of the system to determine the likelihood that personal information has been or will be misused. If the investigation determines the misuse of information has occurred or is reasonably likely to occur, notice must be given as soon as possible to the affected Delaware resident. The law was effective June 28, 2005.

SCHWARTZ & BALLEN LLP

Notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notice may be written, electronic or telephonic. As an alternative, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the individual's website and notification to major statewide media if the cost of providing notice would exceed \$75,000, there are more than 100,000 affected individuals or the individual does not have enough information to provide written, telephonic or electronic notice.

“Personal information” is a Delaware resident's name in combination with one or more of the following data elements when either the name or the data element is not encrypted:

- Social Security number;
- Driver's license or Delaware Identification Card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial account.

An individual that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance or guidelines established by its primary or functional regulator is in compliance with the act if the individual or commercial entity notifies affected residents in accordance with the maintained procedures. Additionally, an individual that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the individual or commercial entity provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the Delaware law.

The State Attorney General is authorized to bring an action to address violations of the act, to ensure compliance and to recover direct economic damages resulting from a violation.

FLORIDA

Florida law (HB 481) (Fla. Stat. ch. 817.568) requires that a person conducting business in the state that maintains computerized data that includes personal information disclose a breach of the security of the system to any Florida resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice is not required if after reasonable investigation the person determines there is no reasonable likelihood of harm to

SCHWARTZ & BALLEN LLP

customers. The determination must be documented in writing and the documentation maintained for five years. The law was effective July 1, 2005.

Written or electronic notice must be given within 45 days following the determination of the breach, consistent with the needs of law enforcement or any measures necessary to determine the presence, nature and scope of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the data collector's website and notification to major statewide media.

"Personal information" is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted:

- Social Security number;
- Driver's license or state identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

A person that maintains notification procedures (1) as part of an information security policy for the treatment of personal information, in which the notification is consistent with the timing requirements of the law or (2) pursuant to the rules, regulations, procedures or guidelines established by the person's primary or functional federal regulator, is deemed to be in compliance with the notification requirements of the law. If a person must notify more than 1,000 persons at a single time, the person must notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

Any person who fails to provide notice in the required 45-day period is subject to a fine of \$1,000 for each day the breach goes undisclosed and after 30 days a \$50,000 fine for each 30 day period, with a maximum of \$500,000. If notification is not made within 180 days, an administrative fine may be imposed of up to \$500,000 per breach.

SCHWARTZ & BALLEN LLP

GEORGIA

Georgia law (SB 230) (Ga. Code Ann. §§ 10-1-910 et seq.) requires an “information broker” that maintains computerized data to provide notice of any breach of the security of the system to any Georgia resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity, security and confidentiality of the system. The law was effective May 5, 2005.

An “information broker” is a person who, for monetary fees or dues, engages in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties.

“Personal information” is an individual’s name in combination with one or more of the following data elements when either the name or data elements are not encrypted or redacted:

- Social Security number;
- Driver’s license or state identification card number;
- Account number or credit or debit card number if the number could be used without additional identifying information, access codes or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of these data elements when not in connection with a person’s name if the information would be sufficient to perform or attempt identity theft from the person whose name was compromised.

Substitute notice may be provided via e-mail, conspicuous posting on the information broker’s website and notification to major statewide media if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the information broker does not have enough information to provide written or electronic notice. In the event that more than 10,000 residents must be notified, the information broker must also notify the nationwide consumer reporting agencies of the timing, distribution and content of the notice.

SCHWARTZ & BALLEN LLP

An information broker that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the information broker provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

ILLINOIS

Illinois law (HB 1633) (Public Act 94-36) requires that a “data collector” that owns or licenses personal information concerning an Illinois resident disclose a breach of the security of the system data to any Illinois resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. A “data collector” is any entity that handles, collects, disseminates or otherwise deals with nonpublic personal information. The law is effective January 1, 2006.

Written or electronic notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity, security and confidentiality of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the data collector does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the data collector’s website and notification to major statewide media.

“Personal information” is an individual’s name in combination with one or more of the following data elements when either the name or the data element is not encrypted or redacted:

- Social Security number;
- Driver’s license or state identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual’s financial account.

A data collector that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the data collector provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

SCHWARTZ & BALLEN LLP

Any data collector who violates the act may be enjoined, subject to restitution, and subject to revocation, forfeiture or suspension of any license, charter, franchise, certificate or other evidence of authority of any person to do business in Illinois. Additionally, a civil fine of up to \$50,000 may be imposed, in addition to a fine of up to \$10,000 for each violation against a person over 65 years old.

LOUISIANA

Louisiana law (SB 205) (La. Rev. Stat. Ann. §§ 3071 et seq.) requires that a person that conducts business in the state or owns or licenses computerized data that includes personal information disclose a breach of the security of the system to any Louisiana resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice is not required if after reasonable investigation the person determines there is no reasonable likelihood of harm to customers. The act will become effective upon adoption of rules by the State Attorney General's Office, but no earlier than January 1, 2006.

Written or electronic notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach, prevent further disclosures and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media.

"Personal information" is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted or redacted:

- Social Security number;
- Driver's license number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

Financial institutions that are subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005 are deemed in compliance with the act. Additionally, a person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides

SCHWARTZ & BALLEN LLP

notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the Louisiana law.

A person may institute an action to recover actual damages resulting from the failure to disclose a breach in a timely matter.

MAINE

Maine law (LD 1671) (Me. Rev. Stat. Ann. tit. 10, §§ 1346 et seq.) requires an “information broker” that maintains computerized data to provide notice of any breach of the security of the system to any Maine resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. An “information broker” is a person who, for monetary fees or dues, engages in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties. The law is effective January 31, 2006.

Written or electronic notice must be made as expeditiously as possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity, security and confidentiality of the data in the system. As an alternative, if the cost of providing notice would exceed \$5,000, there are more than 1,000 affected individuals or the information broker does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the information broker’s website and notification to major statewide media.

“Personal information” is an individual’s name in combination with one or more of the following data elements when either the name or the data element is not encrypted or redacted:

- Social Security number;
- Driver’s license or state identification card number; or
- Account number or credit or debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the above data elements when not in connection with the individual's name if the information, if compromised, would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

SCHWARTZ & BALLEN LLP

If an information broker must notify more than 1,000 persons at a single time, the information broker must notify, without unreasonable delay, all nationwide consumer reporting agencies. Additionally, when notice of a breach is required, the information broker must notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the information broker is not regulated by the department, the Attorney General.

An information broker who violates this act is subject to a fine of up to \$500 per violation up to \$2,500 per day. In addition, injunctive relief may be obtained.

MINNESOTA

Minnesota law (HF 2121) (Minn. Stat. § 325E.61) requires that a person conducting business in the state that owns or licenses computerized data disclose a breach of the security of the system to any Minnesota resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The law is effective January 1, 2006.

Written or electronic notice must be given in the most expedient time possible and without reasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach, to identify individuals affected and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media.

“Personal information” is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted:

- Social Security number;
- Driver's license number or Minnesota identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

SCHWARTZ & BALLEN LLP

The act specifically exempts financial institutions as defined in Title V of the Gramm-Leach-Bliley Act and entities subject to the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996. If a person must notify more than 500 persons at one time, then within 48 hours the person must notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

The State Attorney General is authorized to enforce the act and seek an injunction.

MONTANA

Montana law (HB 732) (Mont. Code Ann. §§ 31-3-115 et seq.) requires that a person conducting business in Montana that owns or licenses computerized data including personal information disclose a breach of the security of the system to any Montana resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The law is effective March 1, 2006.

“Breach of security” is the unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained and causes or is reasonably believed to cause loss or injury to a Montana resident.

Notice must be given without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. Notice may be written, electronic or telephonic. As an alternative, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person’s website or notification to major statewide media if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice.

SCHWARTZ & BALLEEN LLP

“Personal information” is an individual’s name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

If a person discloses a security breach to any individual pursuant to the act and gives notice to the individual that suggests, indicates or implies that the individual may obtain a copy of his or her file from a consumer reporting agency, the person must coordinate with the consumer reporting agency as to the timing, content and distribution of notice to the individual.

A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

Violators are subject to a fine of up to \$10,000 and an injunction against future violations.

NEVADA

Nevada law (SB 347) (Nev. Rev. Stat. 52.18 et seq.) requires that a “data collector” that owns or licenses computerized data that includes personal information disclose a material breach of the security of the system data to any Nevada resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. A “data collector” includes any corporation, financial institution or other business entity that handles, collects, disseminates or otherwise deals with nonpublic personal information. The law is effective January 1, 2006.

Written or electronic notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system data. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the data collector does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known),

SCHWARTZ & BALLEN LLP

conspicuous posting on the data collector's website and notification to major statewide media.

“Personal information” is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted:

- Social Security number or employer identification number;
- Driver's license or identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

The notification provisions specifically exempt data collectors subject to the privacy and security provisions of the Gramm-Leach-Bliley Act. In the event that 1,000 persons must be notified at one time, the data collector shall also notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

A data collector that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the data collector provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

The act provides that any data collector who provides notification pursuant to the act may institute an action for damages, including the costs of notification, against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector, or a court may order restitution upon convicting such a person. The State Attorney General is authorized to enforce the act and seek an injunction.

NEW JERSEY

New Jersey law (AB 4001) (to be codified) requires that a business conducting business in the state that maintains computerized records that include personal information disclose a breach of the security of the system to any New Jersey resident whose unencrypted personal information was or is reasonably believed to have been accessed by an unauthorized person. Notice is not required if the business establishes that misuse of the information is not reasonably possible. Any such determination must be documented in writing and the documentation maintained for five years. The act is effective January 1, 2006.

SCHWARTZ & BALLEN LLP

Written or electronic notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the business does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the business's website and notification to major statewide media.

“Personal information” is an individual's name in linked with one or more of the following data elements:

- Social Security number;
- Driver's license or state identification card number;
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

A business that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the New Jersey law if the business provides notification in accordance with that policy on breach of security and if the notification is consistent with the requirements of the law.

A business that must disclose a breach must report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety prior to notifying customers. Additionally, if a business must notify more than 1,000 consumers at one time, the business must notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

The State Attorney General is authorized to enforce the act and seek an injunction and civil penalties of not more than \$10,000 for the first offense and not more than \$20,000 for the second and each subsequent offense. Additionally, any person injured by violation of the act may institute an action for treble damages.

NEW YORK

New York law (AB 4254/SB 5827) (N.Y. Gen. Bus. Law § 899-aa) requires a person conducting business in the state that owns or licenses computerized data to provide notice of any breach of the security of the system to any New York resident whose unencrypted private information was or is reasonably believed to have been acquired by an unauthorized person. The law is effective December 7, 2005.

SCHWARTZ & BALLEN LLP

In determining whether information has been acquired or is believed to have been acquired, a person may consider indications that (1) the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or device containing information, (2) the information has been downloaded or copied or (3) the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Notice must be given without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Notice may be written, electronic (if the individual expressly consented to receiving notice in electronic form) or telephonic, provided that a log of electronic and telephonic notice must be kept. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written, electronic or telephonic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media.

Notice must include contact information for the person making the notification and a description of the categories of information that were affected by the breach, including specification as to which of the elements of personal information and private information are believed to have been acquired.

"Private information" is "personal information" in combination with one or more of the following data elements when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- Social Security number;
- Driver's license or non-driver identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

"Personal information" is any information concerning a natural person that, because of name, number, personal mark or other identifier, can be used to identify that person.

If a person must notify more than 5,000 New York residents at a single time, the person must notify consumer reporting agencies of the timing, distribution and content of the notice and the approximate number of affected persons. The Attorney General is charged with maintaining a list of consumer reporting agencies.

SCHWARTZ & BALLEN LLP

Additionally, when notice to any New York residents is required, the State Attorney General, the Consumer Protection Board and the State Office of Cyber Security and Critical Infrastructure Coordination must be notified of the timing, distribution and content of the notice and the approximate number of affected individuals.

The State Attorney General is authorized to enforce the act and seek an injunction. Additionally, the court may award damages, including consequential financial losses, to a person entitled to notice if notification was not provided pursuant to the act. If the court determines that a person violated the act knowingly or recklessly, then it may impose a civil penalty of the greater of \$5,000 or \$10 per instance of failed notification up to \$150,000.

NORTH CAROLINA

North Carolina law (SB 1048) (N.C. Gen. Stat. § 75-65) requires that a business that owns or licenses personal information of residents of North Carolina or that conducts business in the state and owns or licenses personal information of consumers in any form (computerized, paper or otherwise) disclose a breach of the security of the system to any affected person whose personal information was acquired by an unauthorized person and unauthorized or illegal use of the personal information has occurred or is reasonably likely to occur. The act is effective December 1, 2005.

Notice must be given without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system. Notice may be written, electronic or telephonic. As an alternative, if the cost of providing notice would exceed \$250,000 or there are more than 500,000 affected individuals, or if the business does not have enough information to provide written or electronic notice or is unable to identify particular affected persons, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the business's website and notification to major statewide media.

Notice must be clear and conspicuous and include a description of:

- The incident in general terms;
- The type of personal information that was subject to the unauthorized access and acquisition;
- The general acts of the business to protect the personal information from further unauthorized access;

SCHWARTZ & BALLEEN LLP

- A telephone number that the consumer may call for further information and assistance, if one exists; and
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

“Personal information” is an individual’s name in combination with one or more of the following:

- Social Security or employer taxpayer identification number;
- Driver’s license, state identification card or passport number;
- Account number or credit or debit card number;
- Personal Identification Code;
- Any other numbers or information that can be used to access a person’s account or financial resources;
- Digital signature;
- Biometric data; or
- Fingerprints.

Financial institutions that are subject to and in compliance with the federal banking agencies’ guidance issued on March 7, 2005 are deemed in compliance with the act.

If a business must notify more than 1,000 consumers at one time, the business must notify, without unreasonable delay, the Consumer Protection Division of the Attorney General’s Office and all nationwide consumer reporting agencies of the timing, distribution and content of the notice.

The State Attorney General is authorized to enforce the act and seek an injunction and a civil penalty of \$5,000 for each violation. Additionally, any person injured by violation of the act may institute an action for treble damages.

NORTH DAKOTA

North Dakota law (SB 2251) (N.D. Cent. Code §§ 12.1-23-11 et seq.) requires that a person conducting business in North Dakota that owns or licenses computerized data including personal information disclose a breach of the security of the system to any North Dakota resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The law was effective June 1, 2005.

Written or electronic notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any

SCHWARTZ & BALLEN LLP

measures necessary to determine the scope of the breach and to restore the integrity of the data system. As an alternative, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice.

"Personal information" is an individual's name in combination with any of the following data elements, when the name and the data elements are not encrypted:

- Social Security number;
- Driver's license number or state identification card number;
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial accounts;
- Date of birth;
- Maiden name of the individual's mother;
- Identification number assigned to the individual by the individual's employer; or
- Digitized or other electronic signature.

The act specifically exempts financial institutions that are subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005. Additionally, a person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

The State Attorney General is authorized to enforce the act and seek an injunction and civil penalties.

RHODE ISLAND

Rhode Island law (H 6191) (R.I. Gen. Laws §§ 11-49.2-1 et seq.) requires that a person conducting business in the state that owns, licenses or maintains data in a system that includes personal information disclose a breach of the security of the system which poses a significant risk of identity theft to any Rhode Island resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice is not required if after reasonable investigation and consultation with law enforcement the person determines there is no reasonable likelihood of harm to customers. The law is effective March 1, 2006.

SCHWARTZ & BALLEN LLP

Written or electronic notice must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$25,000, there are more than 50,000 affected individuals or the person does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media.

“Personal information” is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted:

- Social Security number;
- Driver's license or state identification card number;
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

A person that maintains notification procedures as part of an information security policy for the treatment of personal information in which the notification is consistent with the timing requirements of the law is deemed to be in compliance with the notification requirements of the law. Additionally, a financial institution that is in compliance with the federal banking agencies' guidance issued on March 7, 2005 or rules, regulations, procedures or guidelines established by the institution's functional regulator under the Gramm-Leach-Bliley Act is deemed in compliance with the act.

A person that violates the act is subject to a fine of not more than \$100 per occurrence up to \$25,000.

TENNESSEE

Tennessee law (SB 2220) (Tenn. Code Ann. § 47-18-2107) requires that an “information holder” disclose a breach of the security of the system to any Tennessee resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. An “information holder” includes any person or business conducting business in Tennessee that owns or licenses computerized data that includes personal information. The law was effective July 1, 2005.

Written or electronic notice must be given in the most expedient time possible and without reasonable delay, consistent with the needs of law enforcement or any

SCHWARTZ & BALLEN LLP

measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the information holder does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the information holder's website and notification to major statewide media.

"Personal information" is an individual's name in combination with one or more of the following data elements when either the name or the data element is not encrypted:

- Social Security number;
- Driver's license number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

The act specifically exempts financial institutions subject to the Gramm-Leach-Bliley Act. In the event that 1,000 persons must be notified at one time, the information holder shall also notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

An information holder that maintains notification procedures as part of an information security policy for the treatment of sensitive personal information is deemed to be in compliance with the notification requirements of the law if the information holder provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

A customer who is injured by a violation of the act may institute a civil action to recover damages or enjoin the information holder from further violation.

TEXAS

Texas law (SB 122) (Tex. Bus. & Com. Code Ann. § 48.103) requires that a person conducting business in the state that owns or licenses computerized data that includes sensitive personal information disclose a breach of the security of the system to any Texas resident whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person. The law is effective September 1, 2005.

Written or electronic notice must be given as quickly as possible, consistent with the needs of law enforcement or any measures necessary to determine the scope

SCHWARTZ & BALLEN LLP

of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person's website or notification to major statewide media.

“Sensitive personal information” is an individual's name in combination with one or more of the following data elements when the name and the data element is not encrypted:

- Social Security number;
- Driver's license or government-issued identification number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

A person that maintains notification procedures as part of an information security policy for the treatment of sensitive personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law. If a person must notify more than 10,000 individuals at a single time, the person must notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

Any person who violates the act is subject to a fine of at least \$2,000 but not more than \$50,000 for each violation. The State Attorney General also is authorized to seek an injunction against any person to restrain the violation of the act.

WASHINGTON

Washington law (SB 6043) (Wash. Rev. Code tit. 19) requires that a person conducting business in Washington that owns or licenses computerized data including personal information disclose a breach of the security of the system to any Washington resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice of a technical breach of the security system is not required if it does not seem reasonably likely to subject customers to a risk of criminal activity. The law was effective July 24, 2005.

Written or electronic notice must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. As an alternative, substitute notice may be provided via e-mail

SCHWARTZ & BALLEEN LLP

(if e-mail addresses are known), conspicuous posting on the person's website and notification to major statewide media if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals or the person does not have enough information to provide written or electronic notice.

"Personal information" is an individual's name in combination with any of the following data elements, when the name and the data elements are not encrypted:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.

A customer who is injured by violation of the act may institute a civil action to recover damages. Additionally, any business that violates the act may be enjoined.