

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

December 27, 2006

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 To date, thirty-four states and Puerto Rico have enacted legislation addressing security breaches. Most recently, Michigan enacted legislation, which is pending the governor's approval.

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

ARIZONA

Arizona law (SB 1338) (Ariz. Rev. Stat. § 44-7501) requires that a person doing business in the state that owns or licenses unencrypted computerized data including personal information conduct a reasonable investigation when it becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data in order to promptly determine if there has been a breach of the security system. If the investigation determines a breach in the security system has occurred, notice must be given to the affected individuals. Notice is not required if the investigation determines a breach of the security of the system has not occurred or is not reasonably likely to occur. The law is effective December 31, 2006.

Written, electronic or telephonic notice must be given in the most expedient manner possible and without unreasonable delay, consistent with the needs of law enforcement or any measure necessary to determine the nature and scope of the breach, to identify affected individuals or to restore the reasonable integrity of the

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

SCHWARTZ & BALLEN LLP

data system. As an alternative, if the cost of providing notice would exceed \$50,000, there are more than 100,000 affected persons or the person does not have enough contact information to provide 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 the data element is not encrypted, redacted or otherwise rendered unreadable or unusable:

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

The Arizona law exempts persons subject to the privacy provisions of the Gramm-Leach-Bliley Act or to the Health Insurance Portability and Accountability Act. The law also provides that a person that complies with notification requirements or security breach procedures pursuant to the requirements of the person's primary or functional regulator is deemed in compliance with these requirements.

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 if the person provides notification in compliance with that policy and if the policy is otherwise consistent with the requirements of this section.

The State Attorney General is authorized to enforce the act. The Attorney General may bring an action to obtain actual damages for willful and knowing violations and a civil penalty of no more than \$10,000 per breach or series of breaches of a similar nature discovered in a single investigation.

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.

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 \$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 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

SCHWARTZ & BALLEN LLP

security, confidentiality, or integrity of personal information maintained by the person. The law was effective July 1, 2003.

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.

COLORADO

Colorado law (HB 1119) (Col. Rev. Stat. § 6-1-716) requires that a person conducting business in the state that owns or licenses computerized data that includes personal information conduct a prompt investigation when it becomes aware of a breach of the security of the system to determine the likelihood that unencrypted personal information has been or will be misused. Notice must be given as soon as possible to the affected Colorado residents unless the investigation determines the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. The law is effective September 1, 2006.

SCHWARTZ & BALLEEN LLP

Written, telephonic or electronic notice must be given in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with 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 250,000 affected Colorado residents or the person does not have sufficient contact information to provide 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 the data elements are not encrypted, redacted or the name or element otherwise rendered unreadable or unusable:

- Social Security number;
- Driver's license number 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 a resident's financial account.

A person that is regulated by state or federal law and that maintains procedures for a breach of security pursuant to the requirements of its primary or functional state or federal regulator is deemed to be in compliance with these requirements. 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 if the person provides notification in accordance with that policy and if the notification is otherwise consistent with the timing requirements of this law.

If the person must notify more than 1,000 Colorado residents, the person must notify, without unreasonable delay, all nationwide consumer reporting agencies of the anticipated date of notification and the approximate number of residents who are to be notified. This requirement, however, does not apply to a person subject to Title V of the Gramm-Leach-Bliley Act.

The State Attorney General is authorized to enforce the act. The Attorney General may bring an action to address violations, recover direct economic damages resulting from a violation and for other relief.

SCHWARTZ & BALLEN LLP

CONNECTICUT

Connecticut law (SB 650) (Conn. Gen. Stat. § 36a-701b) 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 was effective January 1, 2006.

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.

SCHWARTZ & BALLEN LLP

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.

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.

SCHWARTZ & BALLEN LLP

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. 817.5681) 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 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.

SCHWARTZ & BALLEN LLP

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 of up to \$500,000 per breach may be imposed.

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

SCHWARTZ & BALLEN LLP

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.

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.

HAWAII

Hawaii law (SB 2290) (to be codified at Haw. Rev. Stat. tit. 26) requires that any business that owns, licenses, maintains or possesses personal information of Hawaii residents or any business conducting business in Hawaii that owns or licenses personal information in any form (whether computerized, paper or otherwise) must provide notice of a breach of unencrypted and unredacted records or data containing personal information to the affected person, where illegal use of the information has occurred or is reasonably likely to occur or that creates a material risk of harm to the person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. The law is effective January 1, 2007.

Written, electronic or telephonic notice must be given without unreasonable delay, consistent with the needs of law enforcement and any measures necessary to determine sufficient contact information, the scope of the breach and to restore the reasonable integrity, security and confidentiality of the system. If cost of the notice would exceed \$250,000, the class of affected persons exceeds 500,000, the business does not have enough contact information or consent to provide written, electronic or telephonic notice, substitute notice may be provided via e-mail, a conspicuous posting on the website of the business and notification to major statewide media for only those persons without sufficient contact information or for unidentifiable affected persons. Notice must include:

- General description of the incident;
- Type of personal information that was subject to the unauthorized access and acquisition;
- General acts of the business to protect from future unauthorized access;
- A telephone number for further information and assistance; and
- Advice directing the affected person to review account statements and monitor free credit reports.

SCHWARTZ & BALLEN LLP

“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:

- Social Security number;
- Driver’s license or Hawaii identification card number; or
- Account number, credit or debit card number, access code or password that would permit access to an individual’s financial account.

If notice must be provided to more than 1,000 people, the business also must notify the State of Hawaii’s office of consumer protection and the nationwide consumer reporting agencies of the timing, distribution and content of the notice.

A financial institution that is in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice is deemed to be in compliance with this requirement. A violation of the act constitutes an unfair or deceptive trade practice under Hawaiian law.

IDAHO

Idaho law (SB 1374) (Idaho Code § 28-51-104 et seq.) requires that a person conducting business in the state that owns or licenses computerized data that includes personal information disclose a breach of the security of the computerized data system to any Idaho resident whose unencrypted personal information was or is reasonably believed to have been misused. Notice is not required if after reasonable and prompt investigation the person determines there is no reasonable likelihood the personal information has been or will be misused. The law is effective July 1, 2006.

Written, electronic or telephonic 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, to identify individuals affected, 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 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.

SCHWARTZ & BALLEN 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 element is 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 a resident’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 data collector provides notification to Idaho residents in accordance with that policy and if the notification is consistent with the timing requirements of the law. A person regulated by state or federal law and that maintains procedures for a breach of security of the system pursuant to the requirements established by law or its primary or functional state or federal regulator is deemed in compliance with the Idaho law if it complies with the maintained procedures when a security breach occurs.

A primary regulator may bring a civil action to enforce compliance with the notice requirements of the Idaho law and to enjoin further violations. Any intentional failure to provide notice under the Idaho law is subject to a fine of not more than \$25,000 per breach of the security of the system.

ILLINOIS

Illinois law (HB 1633, 4198) (815 Ill. Comp. Stat. 530/10) 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. The data collector also must disclose to the consumer the personal information that was obtained as a result of the breach. A “data collector” is any entity that handles, collects, disseminates or otherwise deals with nonpublic personal information. The law was 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

SCHWARTZ & BALLEN LLP

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 and if the notification is consistent with the timing requirements of the law.

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.

INDIANA

Indiana law (H. 1101) (Ind. Code § 24-4.9) requires that a data base owner disclose a breach of the security of a system to any Indiana resident whose unencrypted personal information was or may have been acquired by an unauthorized person or whose encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key, if the data base owner knows, should know or should have known the unauthorized acquisition has resulted or could result in identity deception, identity theft, or fraud affecting the Indiana resident. The law is effective July 1, 2006.

Written, electronic or telephonic notice or notice by facsimile must be given in the most expedient time possible and without unreasonable delay, consistent with the needs of the attorney general or law enforcement, or any measures necessary to discover the scope of the breach or restore the integrity of a computer system. As an alternative, if the cost of providing notice would exceed \$250,000 or there are more than 500,000 affected individuals, substitute notice may be provided by conspicuous

SCHWARTZ & BALLEN LLP

posting on the data base owner's website and notification to major media in the geographic area where the affected state residents reside.

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

- Driver's license number;
- State identification card number;
- Credit card number; or
- Financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account

Financial institutions that comply with the disclosure requirements of the federal banking agencies' guidance issued on March 7, 2005 are deemed in compliance with the act. Additionally, a data base owner that maintains notification procedures as part of an information privacy policy, security policy or compliance plan under certain federal laws, including the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or Patriot Act, is not required to make a disclosure under Indiana law if the data owner's policy requires that Indiana residents be notified of a security breach without unreasonable delay and the data base owner complies with that policy.

If a data base owner must notify more than 1,000 consumers, the data base owner must disclose to each nationwide consumer reporting agency information necessary to assist in preventing fraud, including personal information of the affected Indiana residents.

The State Attorney General is authorized to bring an action to obtain an injunction, a civil penalty of not more than \$150,000 per deceptive act and reasonable costs.

KANSAS

Kansas law (SB 196) (to be codified) requires a person conducting business in the state that owns or licenses computerized data that includes personal information conduct a reasonable and prompt investigation when it becomes aware of any 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 Kansas residents. The law is effective July 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 restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$100,000, there are more than 5,000 affected individuals or the person does not have enough information to provide 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 linked to one or more of the following data elements when the data element is not encrypted or redacted:

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

A person that is regulated by state or federal law and maintains procedures for a breach of security pursuant to the requirements of its primary or functional regulator is deemed to be in compliance with these requirements. 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 these requirements if the person provides notification in accordance with that policy and if the notification is consistent with the timing requirements of this law.

If the person 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 or, for insurance companies licensed to do business in Kansas, the insurance commissioner is authorized to enforce the act. The Attorney General may bring an action at law or equity to address violations and for other appropriate relief.

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

SCHWARTZ & BALLEEN LLP

after reasonable investigation the person determines there is no reasonable likelihood of harm to customers. The act was 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, 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 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; LD 2017) (Me. Rev. Stat. Ann. tit. 10, § 1346 et seq.) requires an “information broker” that maintains computerized data to 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 a state resident's personal information has been or is reasonably believed to have been acquired by an unauthorized person, notice must be given to the affected resident. An “information broker” is a person

SCHWARTZ & BALLEEN LLP

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.

A person other than an information broker who maintain computerized data must 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 that misuse of a state resident's personal information has occurred or if it is reasonably possible misuse will occur, notice must be given to the affected state resident. The law was effective January 31, 2006 as to information brokers and becomes effective January 31, 2007 as to all other persons.

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 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 or state identification card number;
- 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.

Persons that comply with security breach notification requirements of federal or Maine law, rules, regulations, procedures or guidelines are deemed to be in

SCHWARTZ & BALLEN LLP

compliance under this law as long as the notification procedures are at least as protective as under this law.

If a person must notify more than 1,000 persons at a single time, the person must notify, without unreasonable delay, all nationwide consumer reporting agencies and include the date of the breach, estimated number of affected persons, and date the persons were or will be notified of the breach. Additionally, when notice of a breach is required, the person must notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General.

A person 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.

MICHIGAN

Michigan law (SB 0309) (Mich. Comp. Laws § 445.63) requires that a person that owns or licenses data that are included in a database disclose a breach of security to any Michigan resident whose unencrypted and unredacted personal information was accessed and acquired by an unauthorized person, or whose encrypted personal information was accessed and acquired by a person with unauthorized access to the encryption key, unless the person determines that the security breach has not or is not likely to cause substantial loss or injury or identity theft to one or more residents of Michigan. The law was effective December 14, 2006.

Written, electronic or telephonic 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 database. As an alternative, if the cost of providing notice would exceed \$250,000 or there are more than 500,000 affected individuals, 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 a description of the security breach, the type of personal information that was the subject of unauthorized access or use, what the person has done to protect the data from further breaches (if applicable), a telephone number where a recipient may obtain assistance or additional information and a reminder for recipients to remain vigilant for incidents of fraud or identity theft. A person may provide any required notice pursuant to an agreement with another person, so long as it does not conflict with the Michigan requirements.

SCHWARTZ & BALLEN LLP

“Personal information” is an individual’s name linked to one or more of the following:

- Social Security number;
- Driver license number or state personal identification card number; or
- Demand deposit or other financial account number, or credit or debit card number, in combination with any required security code, access code or password that would permit access to any of the resident’s financial accounts.

If the person must notify more than 1,000 Michigan residents, the person must notify, without unreasonable delay, all nationwide consumer reporting agencies of the number of notices provided to Michigan residents and the timing of the notices. Persons subject to title V of the Gramm-Leach-Bliley Act are exempt from this requirement.

Financial institutions subject to and in compliance with the federal banking agencies’ guidance issued on March 7, 2005 or persons subject to and in compliance with HIPAA regulations regarding unauthorized access to customer information are deemed in compliance with the act.

Persons who knowingly fail to provide a required notice may be subject to a civil fine of not more than \$250 per failure, to a maximum of \$750,000. The State Attorney General or other prosecuting attorney may bring an action to recover a civil fine.

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 was 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.

SCHWARTZ & BALLEN 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 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.

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. § 30-14-1704) 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 was 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,

SCHWARTZ & BALLEN LLP

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.

"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.

NEBRASKA

Nebraska law (LB 876) (to be codified) requires a person that owns or licenses computerized data that includes personal information to conduct a reasonable and prompt investigation when it becomes aware of a breach of the security of the system to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines use of information about a Nebraska resident has occurred or is reasonably likely to occur, notice must be given as soon as possible and without unreasonable delay to the affected Nebraska resident. The law is effective July 13, 2006.

SCHWARTZ & BALLEN LLP

Written, telephonic or electronic notice must be given as soon as possible and without unreasonable delay, consistent with the needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the 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 \$75,000, there are more than 100,000 affected Nebraska residents or the person does not have enough information to provide notice. The law includes special substitute notice provisions for small businesses.

“Personal information” means a Nebraska resident's name in combination with one or more of the following data elements when either the name or data elements are not encrypted, redacted or otherwise altered such that the name or data elements are unreadable:

- Social Security number;
- Motor vehicle operator'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;
- Unique electronic identification number or routing code, in combination with any required security code, access code or password; or
- Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.

A person that is regulated by state or federal law and maintains procedures for a breach of security pursuant to the requirements of its primary or functional regulator is deemed to be in compliance with this section if the person notifies affected Nebraska residents in accordance with the maintained procedure. 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 if the person provides notification to Nebraska residents in accordance with that policy and if the notification is consistent with the timing requirements of this law.

The State Attorney General is authorized to issue subpoenas and seek and economic damages for each affected Nebraska resident injured by violations of the law.

NEVADA

Nevada law (SB 347) (Nev. Rev. Stat. § 603A.220) 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

SCHWARTZ & BALLEN LLP

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 was 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), 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.

SCHWARTZ & BALLEN LLP

NEW HAMPSHIRE

New Hampshire law (HB 1660) (N.H. Rev. Stat. Ann. § 359-C:19 et seq.) requires a person doing business in the state who owns or licenses computerized data that includes personal information, to determine the likelihood that personal information has been or will be misused when it becomes aware of a security breach. If misuse has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals. The law is effective January 1, 2007.

Written, electronic, or telephonic notice or notice given pursuant to the person's internal notification procedures as part of an information security policy must be given as soon as possible. Delayed notice is permitted if notification would impede a criminal investigation or jeopardize national or homeland security. As an alternative, if the cost of providing notice would exceed \$5,000, the affected class exceeds 1,000 persons, or there is insufficient contact information or no consent to make written, electronic or telephonic notice, substitute notice may be given by providing e-mail notice (if e-mail addresses are known), conspicuous posting on the person's business website, and notification to major statewide media.

Notice must include a description of the incident, approximate date of the breach, type of personal information obtained as a result of the breach and the telephonic contact information for the person giving 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 elements are not encrypted:

- Social Security number;
- Driver's license number or other government identification number; or
- Account number, credit card number, 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.

Any person which maintains procedures for security breach notification pursuant to state and federal laws shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws.

Financial institutions must notify their primary regulator and all other persons must notify the New Hampshire attorney general's office of timing and distribution of the notices. Additionally, if a person must notify more than 1,000 consumers, the

SCHWARTZ & BALLEN LLP

person must notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

Any person injured by any violation under this subsection may bring an action for actual damages and equitable relief, costs and attorney's fees. The court must award at least two times the actual damages for willful or knowing violations, but no more than treble damages. The New Hampshire attorney general is authorized to enforce this law.

NEW JERSEY

New Jersey law (S1914) (N.J. Stat. Ann. § 56:8-163) 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 was 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. 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' 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.

SCHWARTZ & BALLEN LLP

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 was effective December 7, 2005.

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.

SCHWARTZ & BALLEN LLP

“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.

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

SCHWARTZ & BALLEN LLP

information has occurred or is reasonably likely to occur. The act was 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' 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;
- 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.

SCHWARTZ & BALLEN LLP

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 § 51-30-01 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 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.

SCHWARTZ & BALLEN LLP

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.

OHIO

Ohio law (HB 104) (Ohio Rev. Code Ann. § 1349.19) requires that a person that owns or licenses computerized data that includes personal information disclose a breach of the security of the system which causes or reasonably is believed will cause a material risk of identity theft or other fraud to any Ohio resident whose unencrypted or unredacted personal information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. The law was effective February 17, 2006.

Written, electronic or telephonic notice must be given in the most expedient time possible but in no event later than 45 days following the person's discovery or notification of the breach, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, 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. Businesses with 10 employees or fewer may provide substitute notice where the cost of providing the notices will exceed \$10,000.

"Personal information" is an individual's name in combination with and linked to one or more of the following data elements when the data elements are not encrypted, redacted or altered by any method or technology rendering the data unreadable:

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

SCHWARTZ & BALLEN LLP

The law specifically exempts financial institutions that are required by and are in compliance with federal law or regulations to notify customers of an information security breach. In the event that 1,000 persons must be notified at one time, the person shall also notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

The State Attorney General is authorized to bring a civil action against violators of the law, including for a temporary restraining order, preliminary or permanent injunction, costs and civil penalties in the amount of \$1,000 per day for up to 60 days of noncompliance, \$5,000 per day after 60 days of noncompliance and \$10,000 per day after 90 days of noncompliance.

PENNSYLVANIA

Pennsylvania law (SB 712) (73 Pa. Cons. Stat. § 2302) requires that an entity that maintains, stores or manages computerized data that includes personal information provide notice of any breach of the security of the system to any Pennsylvania resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. An entity also must provide notice of a breach if encrypted information is accessed and acquired in unencrypted form, if the security breach is linked to a breach of the security of the encryption or involves a person with access to the encryption key. The law was effective June 22, 2006.

Written, electronic or telephonic notice must be provided 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 \$100,000, there are more than 175,000 affected individuals or the entity does not have sufficient contact information, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the entity's website and notification to major statewide media.

“Personal information” means an individual's name in combination with and linked to any of the following data elements, when the data elements are not encrypted or redacted:

- Social Security number;
- Driver's license number or state identification card number;
- Financial 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

Financial institutions subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005 or other entities in compliance with requirements of their primary or functional federal regulators are deemed in compliance with the act. Additionally, any entity that maintains notification procedures as part of an information privacy or security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the entity provides notification in accordance with its policies and if the notification is consistent with the timing requirements of the law.

If an entity must notify more than 1,000 persons at one time, the entity must notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution and number of notices.

Violations of this law are deemed to be unfair or deceptive acts or practices, and the Pennsylvania Attorney General has exclusive authority to bring an action under state law.

PUERTO RICO

Puerto Rico law (No. 111) and regulations of the Consumer Affairs Department require persons who own or are custodians of a database for commercial use that includes all or part of a personal information archive to notify citizens of Puerto Rico of any violation of the security of the system whose personal information was not protected with cryptographical codes beyond a password. The law was effective January 19, 2006 and the regulations became effective August 23, 2006.

Written or electronic notice must be given in the most expedient manner, consistent with the needs of law enforcement or any measures necessary to reinstate security to the system. As an alternative, substitute notice may be provided via an informative brochure sent through a postal or electronic mail list, conspicuous posting on the person's website and notification to press media, including a daily newspaper of general circulation if the cost would exceed \$100,000, there are more than 100,000 affected persons, the person does not have enough information to locate the affected persons or identifying them would be too expensive due to the number affected or the economic situation of the company or entity.

The notice must include the needs of any current investigation or court case, nature of the situation, number of clients potentially affected, if criminal complaints have been filed, measures being taken, an estimate of time and cost required to rectify the situation and, if known, how the security breach occurred and what information was breached.

SCHWARTZ & BALLEN LLP

“Personal information archive” is an individual’s name in combination with any of the following data elements, when it can be accessed without a cryptographic code:

- Social Security number;
- Driver’s license number, electoral card or any official identification;
- Numbers of banking or financial accounts, with or without access passwords;
- Names of users and access passwords to computer systems;
- Medical information protected by HIPAA;
- Tax information; or
- Labor evaluations.

Persons must notify the Department of Consumer Affairs within ten (10) days after a system security violation is detected. The Department will make a public announcement on the next working day if the person was unable to identify the affected individuals.

The law will not be interpreted in prejudice of information and security policies the company or entity had in place prior to the effective date of the law that offer equivalent or greater protection to the security of information.

The Secretary of Consumer Affairs may impose fines from \$500 to a maximum of \$5,000 per violation. The law also permits consumers to bring an action for violations.

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 was effective March 1, 2006.

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

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:

- 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 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),

SCHWARTZ & BALLELLP

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 was 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 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

SCHWARTZ & BALLEN LLP

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.

UTAH

Utah law (SB 69) (Utah Code Ann. § 13-42-101) requires that a person who owns or licenses computerized data that includes personal information notify state residents if a reasonable and prompt investigation of a breach of system security reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur. The law is effective January 1, 2007.

Written notice by first-class mail, electronic notice, telephonic notice or notice by publication in a newspaper of general circulation must be given in the most expedient time possible without unreasonable delay, consistent with the needs of law enforcement or measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

“Personal information” means a person's name in combination with one or more of the following data elements when either the name or data element is unencrypted or not protected by another method that renders the data unreadable or unusable:

SCHWARTZ & BALLELLP

- Social Security number;
- Financial account number or credit or debit card number, and any required security code, access code or password that would permit access to the person's account;
- Driver's license number or state identification card number.

The law specifically exempts persons who are regulated by state or federal law and required to maintain security breach procedures if the person notifies affected Utah residents in accordance with the other applicable law.

The State Attorney General is authorized to bring a civil action against violators, including for injunctive relief or a civil fine of no greater than \$2,500 for a violation(s) concerning a specific consumer and no greater than \$100,000 in the aggregate for related violations concerning more than one consumer.

VERMONT

Vermont law (S284) (Vt. Stat. Ann. tit. 9, § 2430 et seq.) requires that any "data collector" that owns or licenses computerized personal information that includes personal information concerning a consumer provide notice of the unauthorized acquisition or access of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the data collector. Notice need not be given if the data collector establishes that misuse is not reasonably possible and provides notice of this determination and an explanation to the State Attorney General or the department of banking, insurance, securities and health care administration, as applicable. The law is effective January 1, 2007.

A "data collector" is an entity that for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

Written, electronic or telephonic notice must be given in the most expedient time possible and without reasonable delay, consistent with the needs of law enforcement agency or any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system. As an alternative, if the cost of notice would exceed \$5,000, the number of persons to be provided written or telephonic notice exceeds 5,000, or the data collector does not have adequate information to provide notice, substitute notice may be given by conspicuous posting on the data collector's website and notification to major statewide media. Notice must include:

- General description of the incident;

SCHWARTZ & BALLEN LLP

- Type of personal information that was subject to the unauthorized access or acquisition;
- General acts of the business to protect from future unauthorized access or acquisition;
- A toll-free telephone number the consumer may call for further information and assistance; and
- Advice directing the affected person to review account statements and monitor free credit reports.

“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, redacted or otherwise rendered unreadable or unusable:

- Social Security number;
- Motor vehicle operator’s license number or nondriver identification card number;
- Financial account number or credit or debit card number, if the numbers can be used without additional identifying information, access codes, or passwords; or
- Account passwords or personal identification numbers or other access codes for a financial account.

If the data collector must notify more than 1,000 persons at one time, the data collector must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notice. Entities licensed or regulated by the department of banking, insurance, securities and health care administration are exempt from this requirement.

A financial institution that is subject to the federal banking agencies’ guidance issued on March 7, 2005 and National Credit Union Administration guidance issued on April 14, 2005 on unauthorized access to customer information are exempt from the law.

The State Attorney General is authorized to investigate, enforce, prosecute, obtain and impose remedies for a violation of the law or regulations promulgated thereunder. The department of banking, insurance, securities and health care administration has authority over entities licensed or registered with that department, however.

SCHWARTZ & BALLEN LLP

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 (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.

WISCONSIN

Wisconsin law (SB 164) (Wis. Stat. § 895.507) requires that an entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin make reasonable efforts to notify an individual (wherever located) if the entity knows the individual's personal

SCHWARTZ & BALLEN LLP

information has been acquired by a person whom the entity has not authorized to acquire it and there is a material risk of identity theft or fraud to the subject. An entity whose principal place of business is not located in Wisconsin must make reasonable efforts to notify each Wisconsin resident if the entity knows personal information pertaining to a state resident has been acquired by a person whom the entity has not authorized to acquire it and there is a material risk of identity theft or fraud to the subject. The law was effective March 31, 2006.

An “entity” is defined as a person, other than an individual, that conducts business in Wisconsin and maintains personal information in the ordinary course of business, licenses personal information in Wisconsin, maintains a depository account for a state resident or lends money to a state resident.

Written notice, notice by a method the entity has previously employed to communicate with the subject, or, if the entity cannot determine the mailing address and has not previously communicated with the subject, notice by a method reasonably calculated to provide actual notice to the subject must be given within a reasonable time consistent with the needs of law enforcement, not to exceed 45 days after the entity learns of the acquisition of personal information. Upon written request by a person receiving the notice, the entity shall identify the personal information acquired.

"Personal information" means an individual's name in combination with, and linked to any of the following data elements if the element is not publicly available and is not encrypted, redacted or altered in a manner that renders the element unreadable:

- Social Security number;
- Driver's license number or state identification card number;
- Financial account number, including a credit or debit card account number, or any security code, access code or password that would permit access to an individual's financial account;
- DNA profile;
- Unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

If an entity must notify 1,000 or more individuals as the result of a single incident, the entity shall without unreasonable delay notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.

The law specifically exempts entities subject to, and in compliance with the Gramm-Leach-Bliley Act or persons with a contractual obligation to such an entity if the entity or person has in effect a policy concerning breaches of information security.

SCHWARTZ & BALLELLP

Copyright © 2006 by Schwartz and Ballen LLP. All rights reserved.