

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

May 23, 2005

To Our Clients and Friends

Re: State Security Breach Laws

Several states have enacted legislation requiring notification to residents of unauthorized disclosures of their personal information. These state laws are described below.

ARKANSAS

Arkansas law (SB 1167) (Ark. Code Ann. § 4-110 et seq.) requires that any person or business 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 or business determines there is no reasonable likelihood of harm to customers. The law is effective August 12, 2005.

Written or electronic notice must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals, or the person or 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 person or business's website and notification to major statewide media.

SCHWARTZ & BALLEEN LLP

“Personal information” is an individual’s name in combination with one or more of the following data elements when either the name or the data 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 or business that maintains notification procedures as part of an information security policy for the treatment of personal information shall be deemed to be in compliance with the notification requirements of the law if the person or business 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 person who violates the act will be guilty of 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 any person or business that conducts 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.

Written or electronic notice must be given upon discovery or notification of the breach in the most expedient time possible and without unreasonable delay. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. As an alternative, if the cost of providing notice would exceed \$250,000, there are more than 500,000 affected individuals, or the person or 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 person or business’s website and notification to major statewide media.

SCHWARTZ & BALLEN LLP

“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 or business that maintains notification procedures as part of an information security policy for the treatment of personal information shall be deemed to be in compliance with the notification requirements of the law if the person or business 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 and may recover a civil penalty of up to \$ 3,000 per violation, reasonable attorney’s fees and costs. Additionally, any business that violates the act may be enjoined from future violations.

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, unless law enforcement determines that the notice will compromise a criminal investigation.

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;

SCHWARTZ & BALLEEN LLP

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

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

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

MONTANA

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

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

Notice must be given without unreasonable delay, consistent with the needs of law enforcement or any measures necessary to determine the scope of the breach and 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 or business's website and notification to major statewide media if the cost of providing notice would exceed

SCHWARTZ & BALLEEN LLP

\$250,000, there are more than 500,000 affected individuals, or the person or business 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 or business 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 business must coordinate with the consumer reporting agency as to the timing, content and distribution of notice to the individual.

A person or business that maintains notification procedures as part of an information security policy for the treatment of personal information shall be deemed to be in compliance with the notification requirements of the law if the person or business 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.

NORTH DAKOTA

North Dakota law (SB 2251) (N.D. Cent. Code § 12.1-23-11 et seq.) requires that any person that conducts 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 is 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 or business’s website and notification to major statewide media if the cost of providing notice would exceed

SCHWARTZ & BALLEN LLP

\$250,000, there are more than 500,000 affected individuals, or the person or business 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, trust companies and credit unions that are subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice. Additionally, a person or business that maintains notification procedures as part of an information security policy for the treatment of personal information shall be deemed to be in compliance with the notification requirements of the law if the person or business 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.

WASHINGTON

Washington law (SB 6043) (2005 Wash. Laws 368) requires that any person or business that conducts business in Washington, which 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 is 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

SCHWARTZ & BALLEEN LLP

measures necessary to determine the scope of the breach and to restore the integrity of the data system. As an alternative, substitute notice may be provided via e-mail (if e-mail addresses are known), conspicuous posting on the person or business'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 or business 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 or business that maintains notification procedures as part of an information security policy for the treatment of personal information shall be deemed to be in compliance with the notification requirements of the law if the person or business 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.

Periodic updates to this memorandum can be found on our website at http://www.schwartzandballen.com/whats_new.html.

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