The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 18895

May 26, 2005

STATE LEGISLATION REQUIRING DISCLOSURE TO CONSUMERS OF BREACH OF SECURITY SYSTEMS IMPLICATING CONSUMERS' PERSONAL INFORMATION

 [18895] May 26, 2005 TO: CLOSED-END INVESTMENT COMPANY MEMBERS No. 33-05 COMPLIANCE MEMBERS No. 3-05 OPERATIONS MEMBERS No. 9-05 PRIVACY ISSUES WORKING GROUP No. 2-05 SEC RULES MEMBERS No. 71-05 SMALL FUNDS MEMBERS No. 51-05 TECHNOLOGY ADVISORY COMMITTEE No. 11-05 RE: STATE LEGISLATION REQUIRING DISCLOSURE TO CONSUMERS OF BREACH OF SECURITY SYSTEMS IMPLICATING CONSUMERS' PERSONAL INFORMATION During this year's state legislative sessions, several states passed laws that require notification to consumers in the event a business experiences a security breach that might implicate a consumer's nonpublic personal information. These bills, which are patterned after a similar law adopted by California in 2002,1 are summarized below. Generally speaking, these laws apply to businesses that conduct business in these states (i.e., have customers in these states) without regard to where the business itself is located. NORTH DAKOTA'S LAW2 REQUIRED DISCLOSURE OF BREACH Effective June 1, 2005, Chapter 51-30 has been added to the North Dakota Century Code. This provision, which may be enforced by the State's Attorney General, requires any person that conducts business in the state and that owns or licenses computerized data that include personal information to disclose any breach of the security of the system following discovery or notification of the breach to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. 1 See Institute Memorandum to Compliance Advisory Committee No. 81-02, Investment Adviser Associate Members No. 24-02, Investment Adviser Members No. 40-02, Primary Contacts-Member Complex No. 80-02, Privacy Issues Working Group No. 6-02, SEC Rules Members No. 84-02, Small Funds Members No. 40-02, and Technology Advisory Committee No. 12-02, dated Oct. 2, 2002. California's law applies to any breach occurring on or after July 1, 2003. 2 A copy of Chapter 51-30, which was enacted as Section 2 of Senate Bill 2251, is available on the North Dakota Assembly's website at: http://www.state.nd.us/lr/assembly/59-2005/bill-text/FRBS0500.pdf. 2 The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. Similarly, if a person maintains, but does not own, computerized data that includes personal information, such

person shall notify the owner of the data if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Any disclosure required by the law may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In such instance, disclosure must be made after the law enforcement agency determines that the notification will not compromise the investigation. METHODS OF NOTICE; ALTERNATIVE NOTIFICATION The notice required by Chapter 51-30 may be provided in writing, electronically, if such electronic notice is consistent with the Federal E-Sign Law (15 USC 7001), or through "substitute notice" if either (1) the cost of providing notice would exceed $250,000, (2) notice must be provided to more than 500,000 persons, or (3) the person providing the notice does not have sufficient contact information. Substitute notice shall consist of each of the following: e-mail notice to each person for whom the business has an e-mail address; conspicuous posting of the notice on the business's website, if the business maintains a website; and notification to major statewide media. In lieu of the above, a business that maintains its own notification procedures as part of an information security policy and is otherwise consistent with the timing requirements of Chapter 51-30 will be deemed to be in compliance with the law's notification requirements if the business notifies subject individuals of a security breach in accordance with its procedures.3 DEFINITIONS As used in Chapter 51-30, the following terms have the following meanings: • "Breach of the Security System" means "unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable." Expressly excluded from this definition is a good-faith acquisition of personal information by an employee or agent of the person if the personal information is not used or subject to further unauthorized disclosure. • "Personal Information" means an individual's unencrypted first name or first initial and last name in combination with any of the following unencrypted data elements: the individual's social security number; a driver's license number; a state identification color photo identification card number assigned by the Department of Transportation; the individual's financial institution 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 accounts; date of birth; maiden name of the individual's mother; an identification number assigned to the individual by the individual's employer; or the individual's digitized 3 A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the North Dakota law. 3 or other electronic signature. Expressly excluded is any publicly available information that is lawfully made available to the general public from federal, state, or local government records. FLORIDA'S LAW4 REQUIRED DISCLOSURE OF BREACH Like North Dakota's law, Section 817.5681 of the Florida Statutes would require any person conducting business in Florida that maintains computerized data that includes personal information to notify any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The timing of such notification differs from that under North Dakota law. While Florida's law would require such notification to be made "without unreasonable delay, consistent with the legitimate needs of law enforcement" it subjects such notice to "any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system." In the absence of authority to delay the notice, Florida's law would require that it be made "no later than 45 days following the determination of the breach." Florida's law would also require any business that maintains computerized data that includes personal information on behalf of another business entity to disclose to the business entity for which the data is maintained a breach

of the system. Such notice must be made as soon as practicable, but no later than 10 days following the determination of breach if personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The law would expressly provide that the business that maintains the data on behalf of another business and that other business can agree on which entity shall provide notice to consumers of the breach. In the event they cannot so agree, the business that has the direct business relationship with the Florida resident must provide the required notice. Notice may be delayed if requested by a law enforcement agent if the agency determines that notice would impede a criminal investigation. The notification periods specified in the bill will commence after the person receives notice from the agency that it will not compromise the investigation. Notwithstanding the above, notice is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local law enforcement agencies, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such determination must be documented in writing and the documentation must be maintained for five years. A person who either fails to document this determination or to maintain such documents for five years may be fined up to $50,000 for such failure. 4 Florida's law, which was enacted as Section 2 of House Bill 481, is available through the website of the Florida Legislature at: http://www.myfloridahouse.gov/loadDoc.aspx?FileName=_h0481er.doc&DocumentType=Bill&BillNumber=0481& Session=2005. 4 Failure to provide the notice required by the law would subject a violator to an administrative fine that is based on the duration of the violation but that shall not exceed $500,000. The maximum fine may be imposed if notice has not been provided within 180 days of being required. METHODS OF NOTICE; ALTERNATIVE NOTIFICATION The methods of notice required by the Florida law, including substitute notice, are substantively similar to those in North Dakota's law. Also, like North Dakota's law, Florida's law provides that a person shall be deemed to be in compliance with the Florida's notification requirements if such person provides notice either pursuant to its own notification procedures that are consistent with the timing requirements of the law or pursuant to the rules, regulations, procedures, or guidelines that are established by the person's primary or functional federal regulator. Unlike North Dakota's law, however, in the event the Florida law would require a person to notify more than 1,000 persons at a single time, the person must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices. DEFINITIONS The definitions in Florida's law, which differ somewhat from those in North Dakota's law, are as follows: • "Breach" or "Breach of the Security of the System" means an "unlawful and unauthorized acquisition" of computerized data "that materially compromises the security, confidentiality, or integrity" of the data. Like North Dakota's definition, the term does not include good faith acquisitions by an employee or an agent so long as such information is not used for a purpose "unrelated to the business or subject to further unauthorized use." • "Personal Information" as defined in Florida's law is limited to an individual's first name, first initial and last name, or middle name and last name in combination with one of the following data elements when such data element is not encrypted: social security number; driver's license number or State identification card 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. The term excludes publicly available information. Florida's law is awaiting the Governor's signature. Once signed, it will have an effective date of July 1, 2005. MONTANA'S LAW5 REQUIRED DISCLOSURE OF BREACH 5 Montana's law, which was enacted as House Bill 732, is available through the website of the Montana Legislature at:

http://data.opi.state.mt.us/bills/2005/billhtml/HB0732.htm. 5 Effective March 1, 2006, Montana law imposes disclosure requirements that are substantively similar to those of North Dakota. Like Florida, however, Montana also permits notice to be delayed consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Montana's law also requires any person or business that maintains, but does not own, computerized data to provide the owner of such data notice of any breach involving personal information METHODS OF NOTICE; SUBSTITUTE NOTICE; ALTERNATIVE NOTIFICATION The notification provisions in Montana's law are identical to those provisions in North Dakota's law, including provisions relating to substitute notice and alternative notification. Unlike North Dakota's law, Montana's law provides that if a business discloses a security breach to any individual pursuant to Montana's law and the notice suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. Such coordination with the consumer reporting agency may not unreasonably delay notice to the affected individuals. RECORD DESTRUCTION In addition to requiring notice of breach, Montana's law requires a business to take all reasonable steps to destroy or arrange for the destruction of a customer's records that are within its custody or control and that contain person information that is no longer necessary to be retained by the business. Such destruction shall be by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. The effective date of this provision is also March 1, 2006. DEFINITIONS As used in Montana's new law, the following terms have the following meanings: • "Records" means any material, regardless of the physical form, on which personal information is stored. It does not include publicly available information or personal information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number. • "Breach of the security of the data system" means the unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisitions by an employee or an agent are expressly excluded from this definition so long as such information is not used or subject to further unauthorized disclosure. • "Personal Information" is defined as an individual's first name, first initial and last name, or middle name and last name in combination with one of the following data elements when either the name or the data elements are not encrypted: social security 6 number; driver's license number or State identification card 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. The term excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records. ARKANSAS' LAW6 Effective August 11, 2005, provisions have been added to Arkansas law that provide for the protection of personal information by requiring that: (1) Arkansas residents receive notice of security breaches; and (2) businesses protect the personal information in their possession from unauthorized access, destruction, use, modification, or disclosure and destroy certain records containing personal information. Any person or business that is regulated under state or federal law that "provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided [by the Arkansas law]" is exempt from the provisions of the Arkansas law. Moreover, "compliance with the state or federal law shall be deemed compliance with the [Arkansas law] with regard to the subjects covered by [such law]." REQUIRED DISCLOSURE OF BREACH With one exception, Arkansas'

law imposes disclosure requirements in the event of a breach that are substantively similar to those of Montana. The one exception is that Arkansas does not require notification if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers. Like other laws discussed above, Arkansas' law requires any person or business that maintains, but does not own, computerized data to provide the owner of such data notice of any breach involving personal information. METHODS OF NOTICE; SUBSTITUTE NOTICE; ALTERNATIVE NOTIFICATION The notification provisions in Arkansas' law are identical to those provisions in Georgia's law, including provisions relating to substitute notice and alternative notification. PROTECTION OF RECORDS Arkansas' law require any person or business that acquires, owns, or licenses personal information about an Arkansas resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. RECORD DESTRUCTION Like Montana's law, the Arkansas law requires a business to take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control 6 A copy of the Arkansas law, which was enacted as Senate Bill 1167, is available on the website of the Arkansas General Assembly at: http://www.arkleg.state.ar.us/ftproot/bills/2005/public/SB1167.pdf. 7 containing personal information that is no longer necessary to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. DEFINITIONS As used in the Arkansas law, the following terms have the following meanings: • "Records" means any material that contains sensitive personal information in electronic form. It does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number. • "Breach of the security of the data system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. It does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure. • "Personal Information" is defined as an individual's first name or first initial and last name in combination with any 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 State identification card number; 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; and medical information. The term excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records. GEORGIA'S LAW7 INFORMATION BROKERS Georgia's new law, Article 34 of Chapter 1 of Title 10 of the Official Code of Georgia, was effective May 5, 2005. Unlike the other state laws discussed above, Georgia's law only applies to "information brokers" or to any person or business that maintains computerized data on behalf of an information broker. "Information broker" is defined in the law to mean: . . . any person or entity who, for monetary fees or dues, engages in whole or in part 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. 7 The Georgia law, which was enacted as Senate Bill 230, is available through the website of the Georgia General Assembly at: http://www.legis.state.ga.us/legis/2005_06/pdf/sb230.pdf. 8 Expressly excluded from the definition are governmental agencies whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes. REQUIRED DISCLOSURE OF BREACH The

provisions in the Georgia law governing the method of notice and providing for substitute notice are substantively identical to those in North Dakota's law. The law also requires any person or business that maintains computerized data on behalf of a data broker to provide the data broker notice of any breach involving personal information. Like North Dakota law, notice may be delayed for the duration of a law enforcement investigation if a law enforcement agency determines that providing notice in the meantime would compromise such investigation. Like Florida's law, Georgia's law requires notice also be provided to consumer reporting agencies, but only if notice would have to be provided to more than 10,000 residents of Georgia at one time. (As noted above, Florida's threshold is notice to more than 1,000 Florida residents.) DEFINITIONS As used in Georgia's law, the following terms have the following meanings: • "Breach of the security of the system" means "unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality, or integrity of personal information of such information maintained by an information broker." Expressly excluded are good faith acquisitions by an employee or agent provided that such information is not used or subject to further unauthorized disclosure. • "Personal information" is defined substantially similar to Florida's definition though it includes in the list of unencrypted information: account passwords or personal identification numbers or other access codes; and any of the items in the list of information "when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to person or attempt to perform identity theft against the person whose information was compromised." • • • • • Tamara K. Salmon Senior Associate Counsel

---