The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 19200

September 28, 2005

STATE LEGISLATION REQUIRING NOTICE TO CONSUMERS OF SECURITY BREACH IMPLICATING THEIR PERSONAL INFORMATION

 [19200] September 28, 2005 TO: CLOSED-END INVESTMENT COMPANY MEMBERS No. 51-05 COMPLIANCE MEMBERS No. 18-05 OPERATIONS MEMBERS No. 14-05 PRIVACY ISSUES WORKING GROUP No. 4-05 SEC RULES MEMBERS No. 107-05 SMALL FUNDS MEMBERS No. 82-05 TECHNOLOGY ADVISORY COMMITTEE No. 20-05 RE: STATE LEGISLATION REQUIRING NOTICE TO CONSUMERS OF SECURITY BREACH IMPLICATING THEIR PERSONAL INFORMATION In May, the Institute notified its members that various states had enacted laws requiring businesses to provide notice to consumers in the event of a security breach that might implicate the consumers' non-public personal information.1 Since that time, fourteen other states have enacted similar laws, which are briefly summarized and compared below.2 1 See Institute Memorandum 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, and Technology Advisory Committee No. 11-05 [18895], dated May 26, 2005 (summarizing the laws enacted by Arkansas, Florida, Georgia, Montana and North Dakota). California enacted a similar law in 2002. 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 [15222], dated Oct. 2, 2002. 2 These states are Connecticut, Delaware, Illinois, Louisiana, Maine, Minnesota, Nevada, New Jersey, New York, North Carolina, Rhode Island, Tennessee, Texas, and Washington. In some of these states, the notification requirements were enacted as part of a broader law on identity theft. The state of Indiana also enacted a law requiring notice of security breaches, but that law pertains only to computerized data maintained by a state or local agency. 2 CONNECTICUT3 NOTIFICATION TO STATE RESIDENTS Effective January 1, 2006, any business that conducts business in Connecticut and, in the ordinary course of business, owns, licenses or maintains computerized data containing personal information must disclose any breach of security to any Connecticut resident whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. (If a business maintains, but does not own, computerized data that includes personal information, notice of the breach must be given to the owner or

licensee of the data). The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, and subject to completion of an investigation by the business to determine the nature and scope of the breach, to identify affected individuals, and to restore the reasonable integrity of the data system. Any required notification may be delayed for a reasonable period of time if a law enforcement agency determines that the disclosure will impede a criminal investigation. The notification must be made after the agency determines that it will not compromise the investigation. The notification outlined above will not be required if, after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the business reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. METHODS OF NOTICE The required notice may be provided in writing; by telephone; electronically, if such notice is consistent with the federal E-Sign law (15 U.S.C. 7001 et seq.); or through "substitute notice." Substitute notice may be used if the cost of providing notice would exceed $250,000; if notice must be provided to more than 500,000 individuals; or if the business does not have sufficient contact information for the affected individuals. Substitute notice consists of all of the following: (1) e-mail notice to each affected individual for whom the business has an e-mail address; (2) conspicuous posting of the notice on the business's website, if one is maintained; and (3) notification to major statewide media, including newspapers, radio and television. ALTERNATIVE NOTIFICATION In lieu of the above, a business that maintains its own notification procedures as part of an information security policy may notify affected individuals of a breach of security in accordance with its procedures if those procedures are consistent with the law's timing requirements. If the business maintains such procedures pursuant to rules or guidelines established by the Securities and Exchange Commission or certain other federal regulators,4 the 3 Connecticut's law, which was enacted as Section 3 of Senate Bill 650, is available through the website of the Connecticut General Assembly at http://www.cga.ct.gov/2005/act/Pa/2005PA-00148-R00SB-00650-PA.htm. 4 They are: the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, and the National Credit Union Administration Board. 3 business will be deemed to be in compliance with the Connecticut law, provided that it gives notice of a breach of security to affected individuals in accordance with those procedures. ENFORCEMENT A violation of the law will constitute an unfair trade practice that can be enforced by the Attorney General. DEFINITIONS • "Breach of security" means unauthorized access to or acquisition of electronic files, media, databases, or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. • "Personal information" means an individual's first name or first initial and last name in combination with one or more of the following data: (1) Social Security number; (2) driver's license number or state identification card number; or (3) 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. Expressly excluded is any publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. DELAWARE5 NOTIFICATION TO STATE RESIDENTS Effective June 28, 2005, any business that conducts business in Delaware and owns or licenses computerized data that contains personal information about a Delaware resident, upon becoming aware of a breach of the security of the system, must in good faith conduct a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that such misuse has occurred or is reasonably

likely to occur, the business must notify affected Delaware residents as soon as possible. (If a business maintains, but does not own or license, computerized data that includes personal information, the business must give notice of a breach to, and cooperate with, the owner or licensee of the data, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur. Cooperation includes sharing information relevant to the breach). The notification must be made 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 computerized data system. Any required notification may be delayed if a law enforcement agency determines that the disclosure will impede a criminal investigation. The 5 Delaware's law was enacted as House Bill 116. The enacted version is not currently available through the website of the Delaware Legislature, but it may be viewed through Lexis-Nexis at 2005 Bill Text DE H.B. 116. 4 required notice must be made in good faith, without unreasonable delay, and as soon as possible after the agency determines that it will no longer impede the investigation. METHODS OF NOTICE These provisions generally track the Connecticut law, except that substitute notice may be used if: (1) the cost of providing notice would exceed $75,000; (2) notice must be provided to more than 100,000 individuals; or (3) the business does not have sufficient contact information for the affected individuals. ALTERNATIVE NOTIFICATION As under the Connecticut law, a business that maintains its own notification procedures as part of an information security policy may notify affected individuals of a security breach in accordance with its procedures if those procedures are consistent with the law's timing requirements. In addition, if the business is regulated by federal or state law and maintains procedures for a breach of the security of the system pursuant to rules or guidelines established by its primary or functional regulator, the business will be deemed to be in compliance with the law's requirements, provided that it notifies affected individuals in accordance with those procedures when a breach occurs. ENFORCEMENT Pursuant to the enforcement duties and powers of the Department of Justice's Consumer Protection Division, the Attorney General may bring an action in law or equity to address violations of this law and for other relief that may be appropriate to ensure proper compliance with these requirements, recover direct economic damages resulting from a violation, or both. DEFINITIONS • "Breach of the security of the system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Expressly excluded from this definition is a good-faith acquisition of personal information by the business's employee or agent for purposes of the business, provided that the personal information is not used or is not subject to further unauthorized disclosure. • "Personal information" means a Delaware resident's first name or first initial and last name in combination with one or more data elements for the resident, when either the name or the data element(s) are not encrypted. The data elements listed in the definition include: (1) Social Security number; (2) driver's license number or state identification card number; or (3) 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 a resident's financial account. Expressly excluded is any publicly available information that is lawfully made available to the general public from federal, state, or local government records. 5 ILLINOIS6 NOTIFICATION TO STATE RESIDENTS Effective January 1, 2006, any "data collector" that owns or licenses personal information concerning an Illinois resident must notify the resident of a breach of the security of the system data following discovery or notification of the breach. (If a data collector maintains, but does not own or license, computerized data that includes personal information, notice of the breach must be given to the owner or licensee of the data, if the personal information was, or is reasonably believed to have been, acquired by an

unauthorized person). The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity, security and confidentiality of the data system. There is no law enforcement exception to the notification requirement. METHODS OF NOTICE These provisions generally track the Connecticut law, except that telephonic notice is not permitted. ALTERNATIVE NOTIFICATION As under the Connecticut law, a business that maintains its own notification procedures as part of an information security policy may notify affected individuals of a security breach in accordance with its procedures if those procedures are consistent with the law's timing requirements. ENFORCEMENT A violation of this law constitutes an unlawful practice under Illinois' Consumer Fraud and Deceptive Business Practices Act. DEFINITIONS • "Breach of the security of the system data" – This definition generally tracks the Delaware law, except that the acquisition of personal information by an employee or agent must be for a legitimate purpose of the business and the personal information may not be used for a purpose unrelated to the business. • "Data collector" – This term is broadly defined to include any privately or publicly held corporation, financial institution, or other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information. • "Personal information" – This definition generally tracks the Delaware law. 6 Illinois' law, which was enacted as House Bill 1633, is available through the website of the Illinois General Assembly at http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036. 6 LOUISIANA7 NOTIFICATION TO STATE RESIDENTS Effective no earlier than January 1, 2006,8 any business that conducts business in the state or that owns or licenses computerized data that includes personal information must, following discovery of a breach of the security of the system containing such data, notify any Louisiana resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (If a business maintains, but does not own or license, computerized data that includes personal information, notice of the breach must be given to the owner or licensee of the data). The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. If a law enforcement agency determines that the required notification would impede a criminal investigation, the notification may be delayed until the agency determines that it would no longer compromise the investigation. The notification outlined above will not be required if, after a reasonable investigation, the business determines that there is no reasonable likelihood of harm to customers. In addition, a financial institution that is subject to and in compliance with the federal interagency guidelines on response programs for unauthorized access to customer information and customer notice will be deemed to be in compliance with the Louisiana law.9 METHODS OF NOTICE These provisions track the Illinois law. ALTERNATIVE NOTIFICATION This provision tracks the Illinois law. 7 Louisiana's law, which was enacted as Senate Bill 205, is available through the website of the Louisiana State Legislature at http://www.legis.state.la.us/billdata/streamdocument.asp?did=320093. 8 While the effective date of the new law is January 1, 2006, its provisions will not take effect until implementing rules are promulgated by the Attorney General's office. 9 See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005) ("Interagency Guidance") (interpretive guidance issued by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision), available at http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/pdf

/05-5980.pdf. 7 ENFORCEMENT A civil action may be instituted to recover actual damages resulting from a failure to disclose to a person in a timely manner that there has been a breach of the security of the system resulting in the disclosure of the person's personal information. DEFINITIONS The definitions for "breach of the security of the system" and "personal information" generally track the Delaware law. MAINE10 Unlike the other state laws discussed in this memorandum, the Maine law applies only to "information brokers" and any person or business that maintains computerized data on behalf of an information broker. "Information broker" is defined as: a person 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. 'Information Broker' does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes. NOTIFICATION TO STATE RESIDENTS Effective January 31, 2006, an information broker that maintains computerized data containing personal information will be subject to notification requirements that generally track those under the Louisiana law, except that the Maine law does not allow the information broker to avoid the notification requirements by determining that the breach poses no reasonable likelihood of harm to customers. The Maine law also requires a person that maintains computerized data on behalf of an information broker to provide the information broker with notice of any breach involving personal information. ADDITIONAL NOTIFICATION REQUIREMENTS Regulators: When notice of a breach is required, the information broker also must notify either the appropriate regulator within Maine's Department of Professional and Financial Regulation or the Attorney General, if the information broker is not regulated by the Department. Consumer Reporting Agencies: If an information broker determines that notification of a breach must be given to more than 1,000 persons at one time, it must also notify consumer reporting agencies (as defined in the federal Fair Credit Reporting Act) that compile and 10 Maine's law, which was enacted as House Bill 1180A, is available through the website of the Maine State Legislature at http://janus.state.me.us/legis/ros/lom/LOM122nd/9Pub351-400/Pub351-400-28.htm#P1036_197584. 8 maintain files on consumers on a nationwide basis. This notice must be made without unreasonable delay. METHODS OF NOTICE These provisions generally track the Illinois law, except that substitute notice may be used if: (1) the cost of providing notice would exceed $5,000; (2) notice must be provided to more than 1,000 individuals; or (3) the business does not have sufficient contact information for the affected individuals. ENFORCEMENT An information broker violating this law is subject to a civil action by the appropriate regulator within the Department of Professional and Financial Regulation or by the Attorney General, if the information broker is not regulated by the Department. Sanctions may include a fine of not more than $500 per violation (up to a maximum of $2,500 for each day the information broker is in violation), equitable relief, or enjoinment from further violations. DEFINITIONS • "Breach of the security of the system" – This definition generally tracks the Delaware law. • "Personal information" – This definition generally tracks the Delaware law, except that the data elements are: (1) Social Security number; (2) driver's license number or state identification card number; (3) account number, or credit or debit card number, if circumstances exist such that the number could be used without additional identifying information, access codes or passwords; (4) account passwords or personal identification numbers or other access codes; or (5) any of the data elements in paragraphs (1)-(4) when not in connection with the individual's first name or first initial and last name, if the information if compromised would be sufficient to permit a person fraudulently to assume or attempt to assume the individual's identity. The definition excludes any publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

MINNESOTA11 NOTIFICATION TO STATE RESIDENTS Effective January 1, 2006, any business that conducts business in the state and that owns or licenses data that includes personal information must disclose any breach of the security of the system to affected state residents. The notification requirements generally track those under 11 Minnesota's law, which was enacted as House Bill 2121, is available through the website of the Minnesota Office of the Revisor of Statutes at http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=SLAW_CHAP&year=2005&session_number=0&cha pter=167. 9 the Louisiana law, except that: (1) a business may not avoid the notification requirements by determining that the breach poses no reasonable likelihood of harm to customers; and (2) the required notification may be delayed only until "a date certain" if a law enforcement agency determines that the notification would impede a criminal investigation. Exempt from this notification requirement, and from the other provisions of the Minnesota law described below, is any "financial institution" as defined in Title V of the Gramm-Leach-Bliley Act.12 ADDITIONAL NOTIFICATION REQUIREMENTS Consumer Reporting Agencies: This provision generally tracks the Maine law, except that notice must be given within 48 hours of discovering circumstances requiring notification and the threshold for using substitute notice is more than 500 persons at one time, as opposed to 1,000 persons under the Maine law. METHODS OF NOTICE These provisions track the Illinois law. ALTERNATIVE NOTIFICATION This provision tracks the Illinois law. ENFORCEMENT The Attorney General has the authority to enforce these provisions. DEFINITIONS The definitions for "breach of the security of the system" and "personal information" generally track the Delaware law. NEVADA13 DUTY TO PROTECT; RECORD DESTRUCTION Effective January 1, 2006, a data collector that maintains records containing personal information of a Nevada resident must implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. In addition, any contract for the disclosure of such personal information maintained by the data collector must include a provision requiring the recipient of the information to 12 "Financial institution" is defined as any institution the business of which is engaging in certain financial activities, including providing investment advisory services. See 15 U.S.C. 6809(3). 13 Nevada's law, which was enacted as Sections 17 through 29 of Senate Bill 347, is available through the website of the Nevada Legislature at http://www.leg.state.nv.us/73rd/bills/SB/SB347_EN.pdf. 10 implement and maintain reasonable security measures as outlined above. If the data collector is in compliance with a federal or state law requiring it to provide greater protection to the records, the data collector will be deemed to be in compliance with these requirements. A data collector also must take reasonable measures to ensure the destruction of records containing personal information concerning its customers once the data collector decides no longer to maintain the records. The records are to be shredded, erased, or otherwise modified so that the personal information in those records is unreadable or undecipherable. NOTIFICATION TO STATE RESIDENTS A data collector that owns, licenses, or maintains computerized data that includes personal information will be required to disclose any breach of the security of the system data to affected state residents. The disclosure requirements generally track those under Louisiana law, except that the Nevada law does not allow the data collector to avoid the notification requirements by determining that the breach poses no reasonable likelihood of harm to state residents.14 A data collector that complies with the privacy and security provisions of the Gramm- Leach-Bliley Act (15 U.S.C. 6801 et seq.) will be deemed to be in compliance with the Nevada law. ADDITIONAL NOTIFICATION REQUIREMENTS Consumer Reporting Agencies: This provision tracks the Maine law. METHODS OF NOTICE These provisions generally track the Illinois law. ALTERNATIVE NOTIFICATION This provision tracks the Illinois law. ENFORCEMENT The Attorney General or any county's District Attorney may seek a

temporary or permanent injunction if he or she has reason to believe that any person is violating, proposes to violate, or has violated the requirements summarized above. DEFINITIONS • “Breach of the security of the system data” – This definition generally tracks the Illinois law, except that the unauthorized acquisition of computerized data must be 14 A data collector who provides the required notification may bring a civil action against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. The damage award could include the reasonable costs of notification, reasonable attorney fees, and punitive damages where appropriate. 11 one that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. • “Data collector” – This definition generally tracks the Illinois law. • “Personal information” – This definition generally tracks the Connecticut law, except that the “publicly available information” exception is broader (i.e., it does not specify that the personal information must be publicly available from federal, state or local government records or from widely distributed media). ENCRYPTION Effective October 1, 2008, a business in Nevada will be prohibited from transferring any personal information of a customer through an electronic transmission (other than a facsimile) to a person “outside of the secure system of the business” unless the business uses encryption to ensure the security of the transmission. NEW JERSEY15 NOTIFICATION TO STATE RESIDENTS Effective January 1, 2006, “any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records” following discovery or notification of the breach to any customer who is a state resident and whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. Similar to the Louisiana law, the disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The required notification must be delayed if a law enforcement agency so requests after determining that the notification would impede a criminal or civil investigation, until such time as the agency informs the business that the notification will not compromise the investigation. Notification of a breach will not be required if the business establishes that misuse of the information is not reasonably possible. Any such determination must be documented in writing and retained for five years. The statute further provides that “any business . . . that compiles or maintains computerized records that include personal information on behalf of another business . . . must notify that business. . . who shall notify its New Jersey customers [as outlined above], of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.” 15 New Jersey’s law, which was enacted as Sections 10-12 and 15 of Assembly Bill 4001, is available through the website of the New Jersey State Legislature at http://www.njleg.state.nj.us/2004/Bills/A3500/4001_R1.PDF. 12 ADDITIONAL NOTIFICATION REQUIREMENTS Law Enforcement: When notice of a breach is required, the business must report the breach and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities. This report must be made in advance of the required customer notifications. Consumer Reporting Agencies: This provision tracks the Maine law. METHODS OF NOTICE These provisions track the Illinois law. ALTERNATIVE NOTIFICATION This provision tracks the Illinois law. RECORD DESTRUCTION Similar to the Nevada law, a business must destroy, or arrange for the destruction of, a customer’s records (as defined below) containing personal information that are within its custody or control if the business no longer will retain them. The records are to be destroyed by shredding, erasing, or

otherwise modifying the personal information in those records so that it is unreadable, undecipherable, or nonreconstructable through generally available means. ENFORCEMENT A willful, knowing, or reckless violation of this law constitutes an unlawful practice under New Jersey's Consumer Fraud Act (N.J. Stat. 56:8-1 et seq.). DEFINITIONS • "Breach of security" – This definition generally tracks the Connecticut law. It also incorporates the good faith exception contained in the definition of "breach of the security of the system data" under the Illinois law. • "Personal information" – This definition tracks the Connecticut law. It further states that dissociated data, if linked, would constitute personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data. • "Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed. 13 NEW YORK16 NOTIFICATION TO STATE RESIDENTS Effective December 7, 2005, any business that conducts business in the state and that owns or licenses computerized data that includes private information must disclose any breach of the security of the system to affected state residents. The notification requirements generally track the Louisiana law, except that the New York law does not allow the business to avoid the notification requirements by determining that the breach poses no reasonable likelihood of harm to customers. The New York law further requires that any notice to state residents (regardless of the method used to provide it, as described below) must include: (1) the business' contact information; and (2) a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, as well as the specific items of personal information and private information were, or are reasonably believed to have been, acquired. ADDITIONAL NOTIFICATION REQUIREMENTS Regulators: When notice of a breach is required as outlined above, the business also must notify the Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination. Consumer Reporting Agencies: This provision generally tracks the Maine law, except that: (1) the threshold is having to provide notification of a breach to more than 5,000 persons at one time; and (2) the law defines "consumer reporting agency" as outlined below.17 METHODS OF NOTICE These provisions generally track the Connecticut law, with the following exceptions. First, to use electronic notice, the state residents receiving notice must have expressly consented to receiving notice in electronic form, such consent must not have been a condition to establishing a business relationship or engaging in any transaction, and the person or business who notifies the state residents must keep a log of each such notice. Second, to use telephonic notice, the person or business that notifies the state residents must keep a log of each such notice. Third, to use substitute notice, a business must demonstrate to the Attorney General that it meets the applicable requirements (i.e., cost to exceed $250,000, notice to more than 500,000 persons, or insufficient contact information for affected residents). 16 New York's law was enacted as Assembly Bill 4254 and concurrently amended by Senate Bill 5827. The enacted versions of these bills are not currently available through the website of the New York State Legislature, but they may be viewed through Lexis-Nexis at 2005 Bill Text NY A.B. 4254 and 2005 Bill Text NY S.B. 5827, respectively. 17 Upon request from any business required to make such notification, the Attorney General will furnish a list of consumer reporting agencies. 14 ENFORCEMENT The State's Attorney General may seek an injunction to halt a violation of these provisions. The court may award damages for actual costs or losses, including consequential financial losses, incurred by a person who was entitled to, but did not receive, notice under these provisions. If the court determines that the business knowingly or recklessly violated this law, it may impose a civil penalty of the greater of

$5,000 or up to $10 per instance of failed notification, to a maximum of $150,000. An action must be brought within two years immediately after "the date of the act complained of or the date of discovery of such act." DEFINITIONS • "Breach of the security of the system" – This definition generally tracks the Delaware law. It further states that, in determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, the business may consider indications that the information: (1) is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; (2) has been downloaded or copied; or (3) was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported. • "Consumer reporting agency" means any person which, for monetary fees, dues or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. • "Personal information" means any information concerning a natural person that, because of name, number, personal mark, or other identifier, can be used to identify such natural person. • "Private information" –This definition generally tracks the definition of "personal information" under the Delaware law. NORTH CAROLINA18 NOTIFICATION TO STATE RESIDENTS Effective December 1, 2005, a business that owns or licenses personal information of North Carolina residents, or any business that conducts business in North Carolina and that owns or licenses personal information in any form (computerized, paper, or otherwise) must provide notice to the affected person that there has been a security breach following discovery or notification of the breach. (If a business possesses records or data containing personal 18 North Carolina's law, which was enacted as part of Section 1 of Senate Bill 1048, is available through the website of the North Carolina General Assembly at http://www.ncga.state.nc.us/Sessions/2005/Bills/Senate/HTML/S1048v6.html. 15 information of North Carolina residents that it does not own or license, or if a business that conducts business in North Carolina possesses records or data containing personal information that the business does not own or license, notice of the breach must be given to the owner or licensee immediately following discovery of the breach). Similar to the Louisiana law, the disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement and with 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. The notice must be clear and conspicuous, and must contain a description of the following: (1) the incident in general terms; (2) the type of personal information that was subject to the unauthorized access and acquisition; (3) the general acts of the business to protect the personal information from further unauthorized access; (4) a telephone number that the person may call for further information and assistance, if one exists; and (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. If a law enforcement agency determines that the required notification may impede a criminal investigation or jeopardize national or homeland security, the notification may be delayed until the agency determines that it would no longer compromise the investigation or jeopardize national or homeland security. If the agency's request to delay notification was not made in writing, the business must contemporaneously document the request, including the name of the law enforcement officer and agency making the request. A financial institution that is subject to and in compliance with the federal interagency guidelines on response programs for unauthorized access to customer information and customer notice will be deemed to be in compliance with the North Carolina law.19 ADDITIONAL NOTIFICATION REQUIREMENTS Consumer Reporting Agencies: This provision

tracks the Maine law. Attorney General: When a business is required to notify consumer reporting agencies, as outlined above, it must also notify the Consumer Protection Division of the Attorney General's office. METHODS OF NOTICE These provisions generally track the Connecticut law, except that: (1) electronic notice may be given only to persons who have agreed to receive communications electronically; (2) telephonic notice may be given only if contact is made directly with the affected persons; and (3) substitute notice may be used only to notify persons for whom the business does not have sufficient contact information or consent or persons whom the business is unable to identify. 19 See Interagency Guidance, at note 9. 16 ENFORCEMENT A violation of this law constitutes a violation of N.C. Gen. Stat. 75-1.1, which declares unlawful any unfair or deceptive practices in or affecting commerce. The law further provides that no individual may bring a private right of action (as permitted by N.C. Gen. Stat. 75-16) unless he or she is injured as a result of the violation. RECORD DESTRUCTION Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a North Carolina resident must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal. These measures must include implementing and monitoring compliance with policies and procedures that require the destruction of papers (or the destruction or erasure of non-paper media) containing personal information so that the information cannot practicably be read or reconstructed. The statute also prescribes how the business may contract with a third party to destroy this information. These provisions do not apply to any bank or financial institution that is subject to, and in compliance with, the privacy and security provisions of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.). DEFINITIONS • "Security breach" means an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. The definition also incorporates the good faith exception contained in the definition of "breach of the security of the system data" under Illinois law. • "Personal information" means a person's first name or first initial and last name in combination with the following identifying information: (1) Social Security number; (2) driver's license number; (3) checking or savings account number; (4) credit or debit card number; (5) personal identification code; (6) digital signature; and (7) any other numbers or information that can be used to access a person's financial resources. Personal information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources. Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records. 17 RHODE ISLAND20 DUTY TO PROTECT Effective March 1, 2006, a business that owns or licenses21 computerized, unencrypted personal information about a Rhode Island resident must implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification, or disclosure. These procedures and practices must be "appropriate to the nature of the information." In addition, a business that discloses personal information pursuant to a contract with a non-affiliated third party must require by contract that the third party implement and maintain such procedures. NOTIFICATION TO STATE RESIDENTS A business that owns, maintains or licenses computerized data that includes personal information must disclose any breach of

the security of the system that poses a significant risk of identity theft to affected state residents. The disclosure requirements generally track the Louisiana law. It also affirmatively requires that notification must be prompt and reasonable following the determination of the breach, unless otherwise provided in the law. A financial institution, trust company, credit union or its affiliates that is subject to and examined for, and found to be in compliance with the federal interagency guidelines on response programs for unauthorized access to customer information and customer notice will be deemed to be in compliance with the Rhode Island law.22 METHODS OF NOTICE These provisions generally track the Illinois law, except that the threshold for using substitute notice is 50,000 individuals. ALTERNATIVE NOTIFICATION These provisions track the Connecticut law. ENFORCEMENT A business that fails promptly to make the notification required by this law will be liable for a civil penalty of not more than $100 per occurrence, with a maximum penalty of $25,000. 20 Rhode Island's law, which was enacted as House Bill 6191, is available through the website of the Rhode Island General Assembly at http://www.rilin.state.ri.us/Billtext/BillText05/HouseText05/H6191Aaa.pdf. 21 The law specifies that "owns and licenses" includes, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. 22 See Interagency Guidance, at note 9. 18 DEFINITIONS The definitions for "breach of the security of the system" and "personal information" generally track the Delaware law. TENNESSEE23 NOTIFICATION TO STATE RESIDENTS Effective July 1, 2005, any information holder must disclose any breach of the security of the system to affected state residents. The notification requirements generally track those under the Louisiana law, except that the Tennessee law does not allow the information holder to avoid the notification requirements by determining that the breach poses no reasonable likelihood of harm to customers. Exempt from this notification requirement, and from the other provisions of the Tennessee law described below, is any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act. ADDITIONAL NOTIFICATION REQUIREMENTS Consumer Reporting Agencies: This provision tracks the Maine law. METHODS OF NOTICE These provisions generally track the Illinois law. ALTERNATIVE NOTIFICATION This provision tracks the Illinois law. ENFORCEMENT Any customer who is injured by a violation of these provisions may bring a civil action to recover damages and to enjoin the business from further violations. DEFINITIONS 23 Tennessee's law, which was enacted as Senate Bill 2220, is available through the website of the Tennessee General Assembly at http://www.legislature.state.tn.us/bills/currentga/Chapter/PC0473.pdf. 19 • "Breach of the security of the system" – This definition tracks the Nevada law. • "Information holder" includes any business that conducts business in Tennessee and that owns or licenses computerized data that includes personal information. • "Personal information" – This definition generally tracks the Delaware law. TEXAS24 DUTY TO PROTECT; RECORD DESTRUCTION Effective September 1, 2005, Texas law places on businesses an affirmative duty to implement and maintain reasonable procedures to protect any sensitive personal information collected in the regular course of business from unlawful use or disclosure. In addition, businesses are required to destroy customer records containing sensitive personal information that will not be retained by the business. The records are to be shredded, erased, or otherwise modified so that the sensitive personal information in those records is unreadable or undecipherable. Exempt from these two requirements is any "financial institution" as defined in Title V of the Gramm-Leach-Bliley Act.25 NOTIFICATION TO STATE RESIDENTS A business that conducts business in the state and owns or licenses computerized data that includes sensitive personal information must disclose any breach of the security of the system to affected state residents. The notification requirements generally track the Louisiana law, except that the Texas law does not allow the business to

avoid the notification requirements by determining that the breach poses no reasonable likelihood of harm to customers. ADDITIONAL NOTIFICATION REQUIREMENTS Consumer Reporting Agencies: This provision generally tracks the Maine law, except that the threshold is having to provide notice to more than 10,000 persons at one time. METHODS OF NOTICE These provisions track the Illinois law. ALTERNATIVE NOTIFICATION 24 Texas' law, which was enacted as Section 2 of Senate Bill 122, is available through the website of the Texas Legislature at http://www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&BILLSUFFIX=00122&VERSION=5&TYPE= B. 25 See note 12. 20 This provision tracks the Illinois law. ENFORCEMENT Any person who violates this law is liable to the State for a civil penalty of at least $2,000 but no more than $50,000 for each violation. In addition to bringing suit to recover the civil penalty owed, the Attorney General may seek injunctive relief against any person who is engaging in, has engaged in or is about to engage in conduct that violates these provisions. The court is authorized to grant equitable relief as appropriate to prevent further violation of the law or any additional harm to a victim of identity theft. DEFINITIONS • "Breach of the security of the system" – This definition tracks the Nevada law. • "Sensitive personal information" – This definition generally tracks the definition of "personal information" in the Delaware law. WASHINGTON26 NOTIFICATION TO STATE RESIDENTS Effective July 24, 2005, any business that conducts business in the state and that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system to affected state residents. No notice is required for any technical breach that does not seem reasonably likely to subject customers to a risk of criminal activity. The notification requirements generally track the Louisiana law, except that the Washington law does not allow the business to avoid the notification requirements by determining that the breach poses no reasonable likelihood of harm to customers. METHODS OF NOTICE These provisions generally track the Illinois law. ALTERNATIVE NOTIFICATION This provision tracks the Illinois law. ENFORCEMENT Any customer injured by a violation of these provisions may institute a civil action to recover damages. The law also states that any business that violates, proposes to violate or has violated these provisions may be enjoined. 26 Washington's law, which was enacted as Section 2 of Senate Bill 6043, is available through the website of the Washington State Legislature at http://www.leg.wa.gov/pub/billinfo/2005- 06/Htm/Bills/Session%20Law%202005/6043-S.SL.htm. 21 DEFINITIONS • "Breach of the security of the system" – This definition tracks the Nevada law. • "Personal information" – This definition generally tracks the Delaware law. Rachel H. Graham Assistant Counsel