COMMENT LETTER

June 14, 2007

Institute Comment Letter on New Jersey's Proposed Consumer Breach and Computer Security System Rules (pdf)

June 14, 2007 Stephen B. Nolan, Action Director Office of the Director New Jersey Division of Consumer Affairs 124 Halsey Street P.O. Box 45027 Newark, NJ 07101 Re: Proposal PRN 2007-116 Relating to the Identity Theft Prevention Act Dear Mr. Nolan: The Investment Company Institute is writing to oppose strongly the Division of Consumer Affairs' (the "Division") adoption of Proposal Number PRN 2007-116, which seeks to implement the provisions of the Identity Theft Prevention Act (the "Act").1 The regulations within this proposal appear both to be inconsistent with the Division's authority under the Act and misguided in seeking to impose a "one-size-fits-all" approach to data security. As a preliminary matter, members of the Institute have long taken seriously their obligation to protect the confidentiality and integrity of non-public consumer information. Indeed, the report recently issued by the President's Identity Theft Task Force, Combating Identity Theft, noted that the federal regulator of the Institute's members, the U.S. Securities and Exchange Commission, "has actively examined securities firms to determine whether they have policies and procedures reasonably 1 The Investment Company Institute ("ICI") is the trade association of the U.S. mutual fund industry. ICI members include 8,781 open-end investment companies (mutual funds), 665 closed-end investment companies, 428 exchange-traded funds, and 4 sponsors of unit investment trusts. Mutual fund members of the ICI have total assets of approximately $10.917 trillion (representing 98 percent of all assets of US mutual funds); these funds serve approximately 93.9 million shareholders in more than 53.8 million households. Because the Institute does not represent the interests of consumer reporting agencies, our comments are directed to the provisions in the proposal relating to breach of security and social security numbers. Mr. Stephan B. Nolan, Acting Director June 14, 2007 Page 2 of 7 designed to protect their customers from identity theft. . . . The SEC has not yet found any deficiencies during its examinations that warranted formal enforcement actions."2 Because of the brevity of time provided to members of the public to comment upon the proposal, our comments are not as specific or extensive as we would prefer. However, we trust they will convey the very serious concerns we have with the ultra vires nature of the proposal and the deleterious impact it will have on our members and other entities, including governmental entities, transacting business in New Jersey. I. THE DIVISION'S AUTHORITY UNDER THE ACT Primary among the Institute's concerns with the Division 's proposal is the fact that, contrary to implementing the Act, it attempts to wholly rewrite the Act's provisions. Indeed, in numerous instances, the implementing regulations bear no rational relationship to the Act. The following discussion amply demonstrates this point. A. Computer Security Requirements Under the guise of

adopting regulations to implement statutory provisions governing providing notice of breach of security to customers, in Regulation 13:45F-3.2 the Division has taken off on a tangent and decided to impose “computer security requirements” that have no nexus to the Act. It bears emphasizing that there is no provision in the Act authorizing the Division – directly or indirectly – to adopt rules regulating the computer security utilized by businesses or public entities. For the reasons discussed below, this proposed regulation is of particular concern to the Institute. 1. The Requirements Apply to Persons Not Subject to the Act To the extent the New Jersey Legislature determines that it is necessary in the public interest to regulate the computer security systems employed by businesses and public entities, it has the authority to enact such requirements subject to constitutions constraints. Surely, if the Legislature intended the Division to adopt computer security standards, it would have either included provisions in the Act governing computer security or directed the Division, as part of §56.8-165, which expressly authorizes the Division to adopt regulations implementing the Act, to adopt regulations governing computer security. In the absence of the Legislature doing so, however, the Division lacks authority under the Act to impose such requirements. This, however, has not stopped the Division from attempting to impose such requirements. Interestingly, a business or public entity that never becomes subject to the Act’s provisions relating to breach of security would be subject to the Division’s regulations implementing 2 See The President’s Identity Theft Task Force, Combating Identity Theft, Volume II: Supplemental Information (April 2007) at p. 13. Mr. Stephan B. Nolan, Acting Director June 14, 2007 Page 3 of 7 these breach provisions because the proposed regulations require “every business and every public entity [to] maintain a security system and security measures covering its computers.” 2. Lack of Evidence Demonstrating the Need for Regulation Proposed Regulation 13:45F-3.2 seems predicated on the notion that the laxity or absence of computer security systems by businesses and public entities warrants the Division mandating computer security system requirements. And yet, there is no evidence in the Division’s proposal that demonstrates – or even discusses – the need for this regulation. Because the Act does not contain any provisions relating to imposing computer security system standards, there is also no legislative documentation regarding the need for this regulation. 3. A Misguided Approach to Regulating Computer Security Not only do we object to proposed Regulation 13:45F-3.2 because it exceeds the Division’s authority and there has been no evidence demonstrating the need for this regulation, but we find this proposed regulation’s approach to computer security to be very misguided. The Division has proposed a “one-size fits all” approach to its state-mandated computer security requirements. While the Division’s proposed computer security requirements appear to be based on the PCI Data Security Standards, it bears noting that such standards were developed for the payment card industry. Notwithstanding, this, the Division proposes to apply the standards developed for the payment card industry to all businesses and public entities without regard to the nature of such business or entity, its size, complexity, the types of records or information it collects and maintains, information security needs, vulnerabilities, or existing system security or the appropriateness of applying the payment card industry’s standards to such entities. We are aware of no other provision under state or federal law that indiscriminately imposes on all businesses and public entities computer security system requirements of the nature proposed by the Division. It also bears noting that, the more standardized security is, the easier it is to defeat, particularly on a large-scale basis. It is for this reason that, for example, the federal Department of Homeland Security has proposed to permit each nuclear facility in the United States to determine its own type and level of security rather than the Department imposing a “one-size-fits-all” standard on each such facility that, when compromised at one facility, is capable of being compromised at all facilities. It seems both inexplicable and naive that the Division would take a less enlightened approach to computer security. To the extent the Legislature ever

authorizes the Division to impose computer security standards on entities, we recommend it be done based on a more principled and meaningful basis rather than by an administrative agency's fiat. Mr. Stephan B. Nolan, Acting Director June 14, 2007 Page 4 of 7 4. The Division's Inadequate Economic Analysis The Division's attempt to impose computer security standards on all businesses and public entities will have far reaching consequences – a major one of which is the costs incurred in implementing these requirements and the disruptions they will cause to current information systems. These costs, which are likely to run into the billions of dollars, are downplayed in the Division's proposal. The extent of the Division's economic analysis of this regulation is as follows: Businesses or public entities that compile or maintain records that include personal information may be subject to increased costs related to establishing and/or maintaining the security of personal information, including the costs for new or updated versions of antiviral software and antisypware. However, many businesses simply may need to activate security features in hardware and software that is already in place on their computer systems and networks. We find this explanation of this provision to be misleading. To begin with, the regulation itself requires "every business and public entity" to be compliant with the regulation without regard to whether it "compile(s) or maintain(s) records that include personal information." Moreover, by implying that an entity may merely "activate security software and antispyware" that is already contained in its existing software and be compliant with Regulation 13:45F-3.2 grossly understates the extensiveness of the regulation's requirements and the burdens compliance with them will impose upon all entities. We are curious as to whether the Division has estimated the costs that it would incur by having to comply with this regulation. If so, those estimates should be part of the public record concerning this proposal. If it has not estimated its own cost, we question the basis for the above economic analysis. 5. The Division's Inspection Authority Interestingly, in its proposal, the Division has granted itself the authority to inspect without cause every business and public entity conducting business in New Jersey. In particular, notwithstanding no such grant of authority to the Division in the Act, proposed Regulation 13:45F- 3.1(a)(1) provides, in relevant part, that every business and public entity must maintain and "keep on file for inspection by the Division . . . the analysis for the system developed by the business or public entity to meet the computer security requirements set forth in N.J.A.C. 13:45F-3.2." In order to conduct an inspection pursuant to this authority, the Division is not required to have any grounds to believe that the business or entity has violated the law or is even believed to have violated the law, nor must the Division satisfy any standard prior to inspecting the entity. It also does not appear from the regulation that the entities subject to the Division's inspection authority are provided any due process rights or considerations prior to or in connection with the Division's inspection. We are extremely Mr. Stephan B. Nolan, Acting Director June 14, 2007 Page 5 of 7 troubled by this unbridled grant of authority to a state agency and note that we are not aware of any other state or federal agency with such sweeping authority. B. Treatment of Encrypted Information Another example of the Division's proposal being contrary to its statutory authority under the Act relates to the Act's definition of "breach of security," which is found in §56:8-161 of the Act. According to the Act, "breach of security" means, in relevant part, unauthorized access to electronic files containing personal information when access to such information "has not been secured by encryption or other method of technology that renders the personal information unreadable or unusable." (Emphasis added.) In other words, according to the plain language of the Act, unauthorized access to encrypted information does not constitute a "breach of security." As such, the provisions in §56:8- 163(a) that requires disclosure of a "breach of security" to any customer whose personal information was subject to unauthorized access does not apply to any breach involving encrypted information. Notwithstanding this, proposed Regulation 13:45F-3.3 requires every business and public

entity to report to the Division of State Police “any breach of security, regardless of encryption . . .” (Emphasis added.) Through provisions such as this, it appears that the Division is attempting – not to implement the Act as written – but to rewrite, through rulemaking, the Act’s provisions in a manner wholly inconsistent with the Act enacted by the Legislature. C. Determining Notice of Breach is Not Required Similarly, the Act provides that disclosure of a breach is not required “if the business or public entity establishes that misuse of the information is not reasonably possible.” According to the Act, any such determination “shall be documented in writing and retained for five years.” This is the extent of the provisions in the Act regarding a business’ or public entity’s obligation to establish that disclosure of a breach is not necessary. Notwithstanding this, proposed Regulation 13:45F-3.4(c) would impose detailed requirements on a business’ or public entity’s determination that misuse of information is not reasonably possible. In particular, the proposed regulation would require the business or public entity to “document, maintain, and make available for inspection by the Division,” the following information: how and by whom the investigation was performed; the basis for the decision that misuse is not reasonably possible, including a summary of the information gathered in making the determination; the levels of security in place and compliance with the proposed regulation’s provisions relating to computer security system requirements; and the extent of the breach. Nothing in the Act appears to authorize the Division to mandate, through rulemaking or otherwise, how a business or public entity goes about the process of determining that disclosure of a security breach is not necessary. Mr. Stephan B. Nolan, Acting Director June 14, 2007 Page 6 of 7 II. SUBSTANTIVE CONCERNS WITH THE REGULATIONS’ PROVISIONS A. The Timing of the Required Notices In addition to our concerns with the Division’s proposed regulations not being consistent with the Act or the Division’s authority under it, we have substantive concerns with many of the provisions in the proposal. Some of our concerns with the provisions relating to computer security systems are discussed above. We are also concerned with the provisions in Regulation 13:45F-3.4, relating to disclosure of breach of security. For example, this rule would require the Division of State Police to be notified of a breach within six hours “following discovery or notification of the breach,” and customers to be notified no more than 24 hours after notification to the Division of State Police. These time frames drastically underestimate the forensic analysis that must be undertaken in the event of a breach. Moreover, within this 30 hour period – even assuming the entity worked, literally, around the clock on this issue, which, too, is unrealistic – the entity would also be required to undertake the investigation contemplated by Regulation 13:45F-3.4(c) to determine whether notification must be provided. This is wholly impractical and demonstrates a lack of understanding of how breaches are discovered, thoroughly investigated, and analyzed and the extensive amount of time this process requires. B. Provisions Relating to the Display of Social Security Numbers The Institute also has concerns with the manner in which the Division has exercised its authority under §56:8-164 of the Act, which prohibits the display of social security numbers. In particular, the provisions of subsection (e), (f), and (g) of proposed Regulation 13:45F-4.1, relating to restrictions on the communication of social security numbers, do not appear to be within the ambit of the Division’s authority under the Act. In particular, while the Act, generally speaking, prohibits the display of social security numbers in certain contexts, subsections (e), (f), and (g) would, respectively, prohibit a person from refusing services to a person who refuses to provide a social security number; require an entity to “state the reason for requesting [an] individual’s Social Security number;” and, request a social security number “in conditions under which the Social Security number will remain confidential.”3 There is nothing in the Act that addresses any of these issues or that authorizes the Division to implement rules going beyond the Act’s provisions. In our experience, states that are desirous of implementing requirements similar

to these have included such provisions in their legislative enactments, not in rules implementing a state's breach law. □ □ □ □ 3 With respect to this last provision, we are uncertain as to what it means or would require of entities subject to it. Mr. Stephan B. Nolan, Acting Director June 14, 2007 Page 7 of 7 As noted above, the brevity of the comment period precludes the Institute from providing more detailed comments on our concerns with the specific provisions within the Division's proposal and their related costs. However, we hope the above comments communicate our very serious and grave concerns with the Division's proposal and why the Institute strongly opposes its adoption. We appreciate the opportunity to share our views with the Division and we hope our comments are given the utmost consideration by the Division during the rulemaking process. If you have any questions concerning these comments, please contact the undersigned by phone (202-326-5825) or email (tamara@ici.org). Sincerely, /s/ Tamara K. Salmon Tamara K. Salmon Senior Associate Counsel

---