NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.
750 First Street N.E., Suite 1140
Washington, D.C. 20002
202/737-0900
Fax: 202/783-3571
www.nasaa.org

NASAA

December 1, 2015

The Honorable Bob Goodlatte
Chairman
House Judiciary Committee
United States House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member
House Judiciary Committee
United States House of Representatives
B-351 Rayburn House Office Building
Washington, DC 20515

Re: December 1, 2015 Hearing on H.R. 699, the Email Privacy Act of 2015

Dear Chairman Goodlatte and Ranking Member Conyers:

On behalf of the North American Securities Administrators Association ("NASAA"),[1] I am writing to express my concern regarding H.R. 699, the Email Privacy Act (the "Act"). This legislation would require a governmental entity, including state securities regulators, to obtain a search warrant before accessing the contents of an electronic communication from an Internet service provider ("ISP"). Currently, 18 U.S.C. § 2703(b) authorizes a governmental entity, after providing a customer notice, to use an administrative subpoena to obtain the contents of a wire or electronic communication from a provider of remote computing service. The Act aims to amend 18 U.S.C § 2703 by prohibiting ISPs from providing to any governmental entity the contents of any communication that is in electronic storage or maintained by the provider without a search warrant.

H.R. 699 as currently drafted could severely hamper regulators' ability to prevent fraud and protect investors.

While NASAA believes it is important to update privacy protections for email and other electronic communications, we are deeply concerned that, as currently constituted, H.R. 699 could severely hamper the ability of state securities regulators, in civil and administrative cases, to prevent securities fraud and assist investors who have been financially harmed. As civil law enforcement agencies, state securities regulators typically rely on subpoenas, not warrants, to obtain critical information for their investigations. In fact, many state regulators have no independent authority to obtain a search warrant from a court. The agencies that do not have independent criminal authority then have no practical way to obtain the warrants that the legislation would require. Criminal law enforcement agencies may not assist in obtaining a warrant if they do not have their own ongoing independent criminal investigation, and there may be legal reasons that prevent the sharing of information between criminal and civil agencies in a parallel investigation. The

[1] The oldest international organization devoted to investor protection, NASAA was organized in 1919. Its membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico, and the U.S. Virgin Islands. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

legislation would effectively foreclose securities regulators from obtaining electronic communications from an ISP in a civil or administrative investigation. The inability to effectively investigate these cases can have a real impact on investor protection, both in hampering the agency's ability to stop an ongoing fraud and in attempting to make investors whole when the fraudulent conduct has been stopped.

Accessing ISP-stored email communications is critical when the target of an investigation has destroyed or refuses to produce email communications.

State securities regulators' concern about the hampering of our investor protection mandate is illustrated by how practice has begun to evolve in the wake of the U.S. Sixth Circuit Court of Appeals decision in 2010, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). In *Warshak*, the court held that the use of a Section 2703(b) subpoena or court order to obtain the contents of emails violated the Fourth Amendment's prohibition against warrantless searches. Following this case, some major ISPs have refused to provide email communications absent a search warrant. In refusing to comply with state administrative subpoenas, those ISPs have continually cited to *Warshak* as the legal basis for not producing email communications. The ISPs cite to *Warshak* whether the emails are older than 180 days or not. While we understand the 180-day cutoff for the mandatory warrant under § 2703(a) for emails in temporary "electronic storage" versus emails older than 180 days under § 2703(b) in "remote computing service" as an attempt to reflect the distinction between opened and unopened email, or email that has been abandoned by the user, the current practice of these ISPs is to withhold all email absent a warrant.

Accessing email communications stored by an ISP is critical in any investigation where the target of the investigation has destroyed or refuses to produce email communications. It is not hard to imagine that an individual who has engaged in conduct that violated the securities law may also be willing to engage in deceptive conduct to obstruct an ongoing investigation. It has been certain regulators' experience that when a target simply has the knowledge that the agency can obtain the same information from an ISP, it prompts compliance with the subpoena from the target. If the target knows that the agency lacks the ability to obtain email communications from an ISP, then the target may be less compliant under the subpoena and engage in conduct that results in the agency being unable to obtain often crucial information in its investigation. In situations where the state securities regulator has no independent ability to obtain a search warrant, under the proposed legislation, crucial information to an investigation will be left out that can result in no action being taken, leaving the perpetrator to continue the scheme, or move on to the next scam, leaving the harmed investors in the wake.

Supreme Court precedent and federal law ensure regulators use their investigative authority appropriately.

Moreover, there currently are safeguards in place to ensure that regulators are not abusing their subpoena authority by arbitrarily combing through massive amounts of emails in search of securities violations. The authority of state securities regulators, and federal agencies, to issue administrative subpoenas to obtain records is limited by U.S. Supreme Court precedent and federal law. All administrative subpoenas can only be issued (1) for a lawfully authorized purpose; (2) seeking only information that is relevant to the inquiry at hand; and (3) containing a specification of the documents to be produced that is adequate, but not excessive, for the purposes of the relevant inquiry.[2] In addition, the current Electronic Communications Privacy Act requires that prior notification of the subpoena be given to the customer, giving the customer an opportunity to contest the subpoena in court. This ability to challenge the administrative subpoena in court is not meaningless as notice is given prior to the production of any records. Further, while search warrants authorize an immediate seizure of records, a subpoena provides an immediate opportunity to challenge the future production of records. The notification provides the recipient

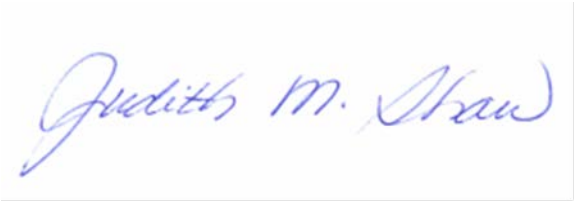
[2] *See Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208-09 (1946).

with the opportunity to petition a court to review the breadth of the subpoena prior to the production of records, as well as the opportunity to negotiate an agreement with the agency that ensures the production of relevant records while minimizing any burden upon the recipient.

Mary Jo White, Chair of the U.S. Securities and Exchange Commission ("SEC"), wrote to express her concerns about the "significant negative impact" that an identical bill to the Email Privacy Act introduced in the Senate in the 113th Congress, S. 607, would have on the SEC's enforcement efforts.[3] In her letter, Chair White suggests that Congress might improve the bill, and strike a better balance between privacy interests and the protection of investors by amending the legislation to establish a "mechanism…to enable a federal civil agency to obtain electronic communications from an ISP for use in a civil enforcement investigation upon satisfying a judicial standard comparable to the one that governs receipt of a criminal warrant." NASAA, similarly, would support such an approach, provided that such a mechanism be fully accessible to state civil agencies, as well as their federal counterparts.

Thank you for your consideration of these concerns. We look forward to working with you as this newly introduced bill moves forward through the legislative process. Should you have any questions, or if NASAA can be of assistance, please contact me or Michael Canning, NASAA's Director of Policy, at (202) 737-0900.

Sincerely,



Judith M. Shaw
NASAA President and Maine Securities Administrator

CC: The Honorable Kevin Yoder
Member of Congress

The Honorable Jared Polis
Member of Congress

[3] Letter from SEC Chair Mary Jo White to Senate Judiciary Committee Chairman Patrick Leahy regarding S. 607, the Electronic Communications Privacy Act Amendments Act of 2013. April 24, 2013. Accessible at https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf