ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Room 4725
Attn: Cybersecurity RFC 2015
Washington, DC 20230

Subj: Comments On Stakeholder Engagement on Cybersecurity in the Digital Ecosystem (Federal Register Notice Vol. 80, No. 53 dated Thursday, March 19, 2015)

Dear Mr. Friedman,

We respectfully write to submit comments on the National Telecommunications and Information Administration's ("NTIA") request for comments regarding Stakeholder Engagement on Cybersecurity in the Digital Ecosystem.

[ABOUT ETA]

ETA's member companies together hold some of Americans' most sensitive financial information, and so we understand the critical importance of strong cybersecurity in the digital age. If personal financial data is left vulnerable and ends up in the hands of hackers or cyber-criminals, it can cause significant material harm for our customers, even when the information was not misappropriated from one of our member companies, but taken in another context and then used to commit ID theft or fraud. We applaud NTIA for gathering information and convening relevant stakeholders in forum to understand potential risks to businesses of all sizes and their customers, in particular in the financial services industry.

If NTIA seeks to narrow the focus of its efforts, ETA believes it would be valuable to prioritize the topics of Web Security and Consumer Trust. To combat the growing threat of identity theft, we must tackle the challenge of authenticating customers in cyberspace. This process will be an opportunity to review the current state of cybersecurity threats and determine whether there are gaps in the policy landscape that could be addressed via a multi-stakeholder-driven code of conduct. A set of best practices in this critical area would help guide businesses of all sizes as they respond to emerging risks and continually adapt to stay one step ahead of the evolving threat landscape. Additionally, the best practices will be fluid enough to take into account the emerging and innovative technologies that develop over time. With new tools in hand, customer-facing businesses could better protect the

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

personal data of their customers from vulnerabilities that lead to identity theft and account takeover.

Finally, if the Multi-Stakeholder Process leads to adoption of consensus recommendations, we believe they must be technology neutral, neither favoring nor condemning any particular technology or security protocol. Businesses know their own risk profile best, and they must continue to have the flexibility and freedom needed to respond to their own unique security challenges. As we have learned, the financial services industry is often first of mind to fraudsters and cyber-criminals due to the nature of the data the industry holds. Despite the commonality of the problem at hand, the solution may be different for each type of financial services company – further illustrating that not every security protocol will be appropriate for every business setting or for every type of data.

Again, we thank the NTIA for its attention to this important issue, and its leadership in attempting to convene interested stakeholders to develop consensus-based codes of conduct. Cybersecurity is too important to consumers and businesses to let this opportunity for dialogue between and amongst stakeholders slip by without making progress understanding the actual nature of threats faced by businesses and consumers, and helping to solve them.

Thank you for your time and attention to this critically important issue.

Sincerely,

Scott Talbott
Senior Vice President for Government Affairs
The Electronic Transactions Association