

April 11, 2011

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554

Re: Comments on Proposed Rulemaking  
Truth in Caller ID Act of 2009  
WC Docket No. 11-39

Dear Ms. Dortch:

I am writing to you in response to Section 10 of the Notice of Proposed Rulemaking regarding the Rule and Regulations Implementing the Truth in Caller ID Act of 2009, requesting comments to assist in the statutorily required report to Congress regard the need for addition legislation in this area. The Truth in Caller ID Act of 2009 alone is not sufficient to protect the nation's financial, social, and security networks from social engineering by Caller ID spoofing.

As Chairman of the Board of the Open Identity Exchange (OIX), the first Open Identity Trust Framework provider, I am particularly concerned with Caller ID spoofing as it related to identity fraud. At OIX, we follow an open market model to provide the certification services needed to deliver the levels of identity assurance and protection needed by communities like the U.S. government, PBS, OCLC, the telco LIDB Forum, and others. OIX applauds the assessment of Congress and the FCC that malicious actors, not the technologies themselves, are the appropriate subjects for regulation. Caller ID spoofing with the intent to "defraud, cause harm, or wrongfully obtain anything of value," however, poses serious financial, social, and security risks that may not be solved by the adjudication of a civil penalty alone.

Productivity loss, harassing calls and social engineering are three of the threats ranging from low to high risks that may occur from Caller ID spoofing. While the Truth in Caller ID Act alone may be enough to deter the two former threats, a more comprehensive study must be done to fully understand the social engineering threats that result from spoofing. The social engineering threats include not only extortion and identity theft, but a growing and increasingly interrelated swath of cyber crimes including computer hacking, intellectual property rights (IPR) issues, economic espionage, and international money laundering.

For example, an increasingly problematic target for social engineering in the financial world is bank call centers. In March 2011 PCI Security Standards Council, the organization responsible for the development, management, education and awareness of data security compliance programs for American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc., released a report citing the growing fraud in the "card-not-present" space. Earlier this year an Australian customer experience research firm revealed around two-thirds of sampled Australian bank call center representatives could be manipulated to divulge

information about other people's accounts. These actions are perfected and celebrated annually at the hacking conference DEF CON's Social Engineering Contest, during which hackers joust for who can obtain the most information from large companies by speaking to customer service representatives.

Caller ID spoofing is a tool for social engineers that threaten the security not only of individual identities, but of our nation's financial pillars, social networks, and national defense. It is for this reason that *OIX urges the FCC include in its report to Congress the recommendation that additional agencies including the Department of Commerce, the Department of Homeland Security, and the Consumer Financial Protection Bureau conduct their own studies on the commercial, national security, and consumer protection impacts of fraudulent Caller ID manipulation.*

*In addition OIX advocates for the FCC to include in its report to Congress the recommendation of a public-private partnership to build industry and government best practices with regard to what constitutes appropriate as well as fraudulent Caller ID actions, and what steps industry can take to facilitate compliance and the enforcement of penalties.*

Congress and the FCC are correct in targeting the actions, not the technology, associated with Caller ID spoofing. But both Congress and the FCC must recognize the even wider role of spoofing as a means to an even greater scope of malevolent actions by social engineers that may compromise Americans' financial, social, and national security. FCC must request Congress enlist the expertise of its fellow agencies in determining the full suite of threats and solutions to Caller ID fraud, and tap the experience and know-how of private sector stakeholders to maximize this regulatory opportunity and ensure that the Truth in Caller ID Act of 2009 serves as watershed legislation for the advancement of cybersecurity in the United States.

Respectfully submitted,

OPEN IDENTITY EXCHANGE

By: /s/ Don Thibeau  
Don Thibeau  
Chairman of the Board,  
Open Identity Exchange  
2400 Camino Ramon, Suite 375  
San Ramon, CA 94583  
202-841-8222