

September 24, 2010

Sent via e-mail

Diane Honeycutt
 National Institute of Standards and Technology
 100 Bureau Drive, Stop 8930
 Gaithersburg, MD 20899
cybertaskforce@doc.gov

The National Business Coalition on E-Commerce and Privacy (“Coalition”) appreciates the opportunity to comment on the Department of Commerce (DOC)’s Notice of Inquiry on Cybersecurity, Innovation, and the Internet Economy.

I. About the Coalition

Founded in February 2000, the Coalition’s membership includes businesses and associations representing diverse economic sectors, including manufacturing, retail, financial services, and media, and it represents their interests before state, federal, and international policy-makers. The Coalition advocates on behalf of mainstream major American businesses and associations in the areas of electronic commerce and privacy.

The 15 major U.S. corporate and association members of the Coalition are traditional, brand name companies now actively using the Internet and new technologies to offer their customers the ability to engage in electronic transactions. Although some of our members are not subject to the Commission’s jurisdiction, the Coalition believes that the FTC’s proposed Principles could well become the basis for an evolving, broader self-regulatory and legislative/regulatory framework affecting all business entities that engage in online advertising, including those not now subject to the FTC’s jurisdiction.

II. General Comments

We wholeheartedly support the Department’s efforts to enhance commercial cybersecurity practices in the non-critical infrastructure and key resources sectors. We also welcome the creation of the Internet Policy Task Force (“Task Force”) and support the Task Force’s efforts to promote conduct by businesses and consumers that will sustain growth in the Internet economy and improve Internet security and its efforts to improve the ability of businesses and consumers to keep pace with ever-evolving cybersecurity risks.

Axiom Corporation
 Affinion Group
 Assurant, Inc.
 Bank of America
 Charles Schwab
 and Co.
 Deere & Company
 Experian
 Fidelity Investments
 Fiserv
 General Motors
 Corporation
 Investment
 Company Institute
 JPMorgan Chase
 and Co.
 Principal Financial
 Group
 The Vanguard
 Group
 Visa Inc.

But we also believe that the Commerce Department could make a great contribution to enhancing cybersecurity nationally by championing efforts by the Federal Government to establish – and enforce -- best practices applicable to the cybersecurity in effect within its own departments and agencies, such that it leads by example and establishes leading standards that the private sector should attempt to replicate. As it is, Americans are much more at risk from cyber breaches resulting from imperfections in government practices and procedures than they are because of cybersecurity deficiencies in the private sector.

In that regard, we feel very strongly that, as practical matter, a static, “one-size fits all” approach to cybersecurity is simply unworkable. That is not to say that underlying principals should not be harmonized; it is the actual implementing mandates that have to bend to the diversity of individualized need and business model. The size, complexity, the types of records or information that various business entities collect and maintain, their information security needs, vulnerabilities, and existing system security are all different and should always be taken into account when constructing the compliance regime by which they will be judged. Private businesses like ours take very seriously their obligation to protect the confidentiality and integrity of non-public information pertaining to consumers, and this obligation is reinforced by the brand risks and liability exposure sure to ensue of they are negligent, with their actions resulting in identifiable harm to their customers. This is not the case with the federal government. There is no liability or brand name risk to be concerned about, and the names of those responsible for breaches are rarely, if ever, made public.

For example, in November, 2007, the Securities and Exchange Commission (SEC) was roundly criticized by the Government Accounting Office (GAO) for its “significant deficienc[ies]” in its information security control practices and policies. Again, in 2008, the SEC’s Office of Inspector General (OIG) published a report that expressed the same concerns, listing a series of findings. If private companies had been found guilty of the same omissions, the liability imposed by the government on them would be costly and damaging, but the SEC (as well as other federal agencies) puts many more people at risk -- and nothing happens. Here are no transparent consequences when government policies and procedures are to blame.

It also bears noting that standardized security is easier to defeat, particularly on a large-scale basis. It is for this reason that, for example, the 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

Axiom Corporation
 Affinion Group
 Assurant, Inc.
 Bank of America
 Charles Schwab
 and Co.
 Deere & Company
 Experian
 Fidelity Investments
 Fiserv
 General Motors
 Corporation
 Investment
 Company Institute
 JPMorgan Chase
 and Co.
 Principal Financial
 Group
 The Vanguard
 Group
 Visa Inc.

facilities. It seems both inexplicable and naive that the Executive Branch would take any less enlightened approach to computer security generally. It should ensure that any policy on cybersecurity takes into account the size of the entities involved, how critically sensitive the information is, over which they have responsibility, and the extent of their vulnerabilities and their resources.

Responses to Specific Questions

- **Quantifying the Economic Impact.** The Coalition is aware of the escalating nature of cybercrime in the United States and its obvious impact on an already faltering economy. According to the Internet Crime Complaint Center (IC3), in a report issued on March 12th of this year, the dollar loss from all cases of crime referred to law enforcement totaled \$559.7 million, compared with \$264.6 million in 2008, a jump of 112%. And this figure does not include the many cases that are never reported or which otherwise never make their way to the attention of law enforcement or regulatory agencies. It is quite likely that many cyberattacks go unreported altogether.

It is well known that some 46 states have adopted data security statutes, and virtually all of them are narrowly tailored to address the need for data security and appropriate notice to affected consumers. One of the questions posed by the NOI is whether there are adequate incentives in place to encourage businesses to provide information about computer hacking and/or serious security breaches. One important way to foster that kind of proactive conduct is for the Congress to enact narrow, preemptive federal law that requires all entities that have custody over non-public personal information to conform to a uniform set of federal data security and notice requirements.

The Coalition has long supported such legislation, but it has consistently failed to be enacted because of an absence of the legislative discipline necessary to keep the bills clean and narrowly focused on data security, rather than on more controversial “data broker” and online privacy issues. It will probably take the encouragement of the Department to assure the enactment of the uniform data security and notification protection consumers deserve, one that focuses on protecting consumer data and notifying them in the event of breaches that create a very real risk of identity theft. In so doing, Congress and the Executive Branch must understand that litigative overkill can – and does – have a counterproductive economic impact. Legislation providing for broad liability exposure through multiple suits on the same facts at the same time in different jurisdictions, often motivated more by the desire to coerce a settlement than by a desire to punish a deserving bad actor, is not the best

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab
and Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors
Corporation
Investment
Company Institute
JPMorgan Chase
and Co.
Principal Financial
Group
The Vanguard
Group
Visa Inc.

approach to what is a very complicated problem. There has to be balance and predictability in enforcement, and those themes should dominate any such legislation.

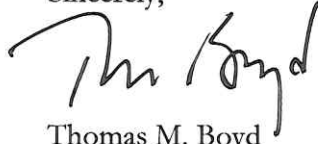
- Raising Awareness.*** The education of consumers about the risks of online commerce has been a central theme for the Coalition's members for some time. Their brands and their businesses depend on it. We encourage the efforts of the National Cyber Security Alliance to educate consumers through their Stay Safe Online campaign, and we agree with President Obama's May, 2009, call for broader public participation in protecting cyberspace. No longer are risks to cybersecurity limited to identifiable segments of online commerce. The whole Internet is a target for both domestic and international fraud as well as Intellectual and Internet espionage. The Department, therefore, should encourage businesses to selectively share their suspicions and their internal intelligence with law enforcement, recognizing that in order to have useful intelligence, businesses should, as a matter of public policy, be provided with liability from disclosure under both the Freedom of Information Act (FOIA) and the possible use and subsequent use of that information in civil litigation.
- Global Engagement.*** We applaud the efforts of national law enforcement officials to increase their collective efforts to engage their global partners in meaningful cybersecurity enforcement. We recognize the need to continue to increase this collaboration to more effectively identify and trace attacks and disable threatening sites. Increased partnership of international law enforcement is critical to ensure fraudsters face criminal charges for their crimes and receive appropriate sentencing. Similarly, as countries enact legislation to strengthen the protections afforded consumers and citizens generally, we believe it is critical that United States officials demand consistency of enforcement so as to discourage the creation, from lack of enforcement, of safe havens within countries, where cyberthieves or hackers can operate free of prosecution. Moreover, when encouraging these steps, we urge law enforcement officials to recognize that enforcement, whether regulatory, criminal and/or civil, must be consistently applied, with the consequences for illegal conduct just as harsh in Europe, the Middle East and Asia as it is in the United States, and conversely.

In closing, we would like to reiterate our support for the Department of Commerce's review of cybersecurity challenges and innovation and the creation of the Internet Policy Task Force.

Axiom Corporation
 Affinion Group
 Assurant, Inc.
 Bank of America
 Charles Schwab
 and Co.
 Deere & Company
 Experian
 Fidelity Investments
 Fiserv
 General Motors
 Corporation
 Investment
 Company Institute
 JPMorgan Chase
 and Co.
 Principal Financial
 Group
 The Vanguard
 Group
 Visa Inc.

Thank you for your consideration of our comments.

Sincerely,



Thomas M. Boyd
Counsel

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab
and Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors
Corporation
Investment
Company Institute
JPMorgan Chase
and Co.
Principal Financial
Group
The Vanguard
Group
Visa Inc.