

**THE NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY**

**STATEMENT**

**OF**

**THOMAS M. BOYD**

**COUNSEL**

**NATIONAL BUSINESS COALITION ON E-COMMERCE & PRIVACY**

**ON**

**H.R. 3997**

**THE FINANCIAL DATA PROTECTION ACT OF 2005**

**BEFORE**

**THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS  
AND CONSUMER CREDIT**

**FINANCIAL SERVICES COMMITTEE  
UNITED STATES HOUSE OF REPRESENTATIVES  
WASHINGTON, D.C.**

**NOVEMBER 9, 2005**

We want to thank Chairman Bachus, Ranking Member Sanders, and the Members of the Subcommittee for inviting us to submit written testimony to you as part of your hearing on H.R. 3997, The Financial Data Protection Act of 2005, and for working with us throughout the process on this important legislation.

My name is Thomas M. Boyd and I am a partner in the law firm of Alston & Bird, LLP. We are counsel to the National Business Coalition on E-Commerce and Privacy ("The Coalition"), a formal, non-profit corporation created in February, 2000. Comprised of seventeen brand name companies, the Coalition is a deliberately diversified organization committed to the adoption of balanced and reasonable national public policy in the area of electronic commerce and privacy. Our members, listed in the margin of this statement,<sup>1</sup> are both financial and non-financial companies and each of them is strongly

<sup>1</sup> J.P. Morgan Chase & Co. and MasterCard Incorporated are recent additions to the Coalition membership.

ACXIOM  
AMERICAN CENTURY INVESTMENTS  
ASSURANT, INC.  
CHECKFREE  
CIGNA  
DEERE & COMPANY  
EASTMAN KODAK COMPANY  
EXPERIAN  
FIDELITY INVESTMENTS  
GENERAL ELECTRIC  
GENERAL MOTORS  
INVESTMENT COMPANY INSTITUTE  
MBNA AMERICA  
PROCTER & GAMBLE  
CHARLES SCHWAB AND CO.

KIM QUISH  
CHAIR

601 PENNSYLVANIA AVENUE, N.W.  
NORTH BUILDING, 10TH FLOOR  
WASHINGTON, DC 20004-2601 USA  
202.756.3385  
FAX - 202.756.3333

committed to ensuring the privacy and security of its customers, both online and offline.

In addition to our membership, we have worked informally with an equally diverse range of other companies, associations and groups for the collective purpose of serving as a positive resource to assist the Financial Services Committee and the Congress in its effort to forge legislation that is designed to protect consumers by establishing national standards for data security and notification. We applaud the work of this Committee and, especially, the cosponsors of H.R. 3997, for their attention to our views throughout the preparation of this legislation. The approach taken by H.R. 3997 to the issue of data security and breach notification is, we believe, consistent with the kind of narrowly tailored, targeted legislation that we believe ought to be the objective of Congressional action in this area. A broader bill, one that incorporates non-germane and unrelated subjects into the data security debate, will inevitably distract from the goal of responding to the absence of federal law that we and our members believe needs to occur sooner rather than later.

As the Chairman and the Subcommittee know, the issues of data security and notification are unusual in that very similar bills have been and are currently under consideration by no less than six Congressional Committees. In the Senate, the Senate Commerce Committee has already reported its bill, S. 1408, and the Senate Judiciary Committee responded by reporting S. 1326, a bill introduced by Senator Jeff Sessions (R-AL). The Senate Banking Committee has held hearings, the most recent of which took place on September 22, and has also promised legislative action. Moreover, due to the inclusion of unrelated matters in S. 1408, such as restrictions on the sale and use of social security numbers, along with language mandating credit freezes, Senate Finance Chairman Charles Grassley (R-IA) has publicly expressed an interest in examining at least the social security component of S. 1408.

In the House, this Committee was the first to act, introducing an earlier version of this legislation, H.R. 3375. The House Commerce Committee has followed with the recent introduction H.R. 4127, reporting it out of Subcommittee last week. Finally, the House Judiciary Committee, like its Senate counterpart, has expressed an interest in acting on this subject as well.

### **Principles to be Employed in Federal Data Security Legislation**

The Coalition recognizes that having so many Congressional Committees engaged in this debate represents a public recognition that the series of data breaches that have taken place during the past year has threatened the confidence that consumers have in businesses that have custody of sensitive personal information pertaining to them. We believe that there is therefore a pressing need for Congress to address deficiencies in the law that currently fail to adequately regulate the interstate application of uniform national standards for data security and, in the event of a

breach of that security, the timely notification of a breach to consumers so they can protect themselves from the potential risk of identity theft. It is not in the interest of the public to expand the impact of such legislation into unrelated and more controversial subjects.

In the course of our deliberations, we have identified a series of principles which we believe ought to be incorporated into any legislation this area that the Congress ultimately enacts.

1. **Preemption.** Starting with the passage, in 2003, of California's data breach and notification legislation (SB 1386, codified as sec. 1798.29 and 1798.82 of the California Civil Code), twenty-one other states – and one municipality – have adopted variations on that original theme. But they are far from alike. New Jersey's new law (A. 4001), like California's, has a fairly low breach notification trigger, and other states vary on how they define the operative terms of their respective statutes. These terms include "personal information", what constitutes a "security breach", and the conditions which would give rise to a mandatory obligation to provide notice of a breach, such as "unauthorized acquisition" of data, or "acquisition" that creates a "risk of identity theft". States have also differed in their treatment of the scope of data containing sensitive personal information and whether it pertains only to electronic data or paper data, whether the applicable data is computerized, unencrypted or encrypted, or redacted or unredacted. For example, New York State's new law covers computerized data pertaining to personal information, including encrypted data if the encryption key has also been acquired. But the New York City ordinance goes even further, expanding the scope of covered information to include unique biometric data as well as electronic signatures, paper as well as computerized data, whether encrypted or not. In North Carolina, the new law would cover data containing "personal information in any form (whether computerized, paper, or otherwise)", which raises the possibility, by use of the word "otherwise", that even oral statements containing personal information may be subject to regulation under the same law.

Our members are all companies servicing a national and often international clientele. The prospect of an ever-changing patchwork of inconsistent state laws can only have one public policy consequence, and that is to confuse and discourage the use by consumers of the Internet and e-commerce generally. Since there are also more than 100,000 municipalities potentially eligible to follow New York City as a participant in this public policy debate, it should be clear why we believe Congress needs to enact a federal, preemptive statute that provides for the uniform application of national standards.

That said, we are aware that some interests, including, among others, the National Association of Attorneys General ("NAAG"), differ with this position, preferring a state by state approach and arguing that states are and should be allowed to remain "laboratories" in which laws pertaining to data breach and security should

be tested. We obviously disagree and suggest that the objectivity of some of these critics may be compromised by their own interest in preserving their jurisdictional turf. To us, it seems self-evident that nothing is more interstate in nature – and therefore within the Constitutional province of the Congress to act – than the computerized transmission of data. Even a federal floor for law in this area, advocated by some, would have no practical effect other than merely to create a different sort of "patchwork" of ever-shifting compliance obligations. Online and offline commerce alike would inevitably suffer from either a federal floor, which states – and localities, for that matter – could exceed, or, as the NAAG and others propose, the simple addition of a federal standard to the potential of 50 different state standards. For businesses such as our members, a regulatory regime like this would be a compliance nightmare, a game of regulatory "gotcha", with consumers in different states subject to different protections, depending exclusively on where, by chance, they happen to live.

We therefore applaud the preemptive provisions of H.R. 3997. They seek to recognize the critical national importance of consistent enforcement and reliable consumer expectations, as well as the reality that a federal bill without meaningful preemption is of little public policy value and only serves to further complicate the enforcement landscape that companies like those we represent have to face.

2. **National Security Standard.** In 1999, the Congress concluded a decade of debate with the historic enactment of the Gramm-Leach-Bliley Act ("GLB"). In section 501(b) of GLB, "financial institutions" were specifically required to implement appropriate "administrative, technical, and physical safeguards" designed to protect the security and integrity of personal information pertaining to their customers. The regulations that followed recognized and underscored that obligation, and it was based on GLB's requirements that some states began to expand a similar obligation to non-financial institutions. Our membership, as we noted earlier, is a diverse one, and just as we have among our members financial institutions such as Charles Schwab & Co., CIGNA, Fidelity Investments, Assurant, CheckFree, JPMorgan Chase, American Century Investments and MasterCard, we also have, as members, non-financial companies such as The Procter & Gamble Company and Eastman Kodak. We also recognize that, in the wake of GLB, a growing number of companies, best known, perhaps, as non-financial companies, also have as part of their corporate structure financial components that are already subject to GLB-based regulation. Examples of such hybrid obligations among our members include Deere & Co., General Electric Company and General Motors.

The Coalition therefore supports legislation, such as HR 3997, that expands, nationwide, the obligation to provide for the security of personal data to include non-financial institutions as well as financial institutions. We believe that the obligation to provide satisfactory security should not generate an industry specific solution but, rather, follow the data, with an appreciation for the differences in business models.

There are, of course, variations in the capacity of different businesses to provide appropriate security for sensitive personal data, and we recommend that, like functional regulators in the case of financial institutions, the Federal Trade Commission ("FTC") is the appropriate regulator to assure that non-financial companies provide security that is "similar to" that which financial institutions are obligated to provide and appropriate for their size and capacity.

H.R. 3997 fulfills this obligation, and establishes an affirmative obligation on all businesses to provide "reasonable policies and procedures to protect the security and confidentiality" of sensitive personal information pertaining to consumers.

3. **Reasonable Notification Trigger.** When GLB was enacted, section 502(b) obligated financial institutions to provide notices to consumers that were designed to inform them that they had the right to "opt out" of allowing companies to share "nonpublic personal information" pertaining to them with third parties. In its review of the effectiveness of this notice requirement, following enactment of GLB, the FTC found that 98% of recipients failed to read the notices, much less act upon them. In the course of the development of this legislation, Congress therefore has the unusual benefit of hindsight, and we therefore know, in advance, that notifications that are not tied to an actual, actionable threat to the consumer are probably destined, like all but 2% of the GLB privacy notices, to be discarded with the weekly trash. We therefore believe the California style notification standard of "unauthorized acquisition" is far too low and will lead, inevitably, to over-notification, which, in turn, defeats the underlying purpose of a notification regime. In that context, it is worth noting that since July 1, 2003, when the California statute became effective, the California Office of Privacy Protection ("OPP") has tracked 83 reported breaches in that state, from a wide range of sources. As of February of this year, Joanne McNabb, the chief of OPP, reportedly was unable to link more than one of what were then 45 breaches to an instance of identity theft related to one of the consumers about whom the breached information applied. However, Ms. McNabb has since stopped trying to apply a link to any of the subsequent 38 breaches that have been reported in California.

It is equally important, though, to remember that companies are always free to unilaterally provide notices whenever they believe it is appropriate to do so, and market competition in this area always plays a dominant role, especially for companies, like members of the Coalition, who view themselves as responsible custodians of personally sensitive information pertaining to their customers. That said, it is an altogether different matter for the federal government to establish a mandate for custodians of sensitive personal information that will inevitably result in a notification regime unrelated to harm or any significant threat of harm. We are aware that some policymakers prefer notice any time a breach occurs, notwithstanding its likely impact on consumers. We believe this approach is unwise and, if embraced, will likely defeat the express purpose of a notification regime by

over-notifying consumers in such a way that we know, by virtue of the GLB privacy notice example, that they will very likely discard those notices to their disadvantage. As FTC Commissioner Leary noted in his testimony before the Senate Commerce Committee on June 16, 2005, such a legislative imperative would likely create a result akin to that which occurs in Aesop's well-known fable, "The Boy Who Cried Wolf."

Earlier this year, the Federal Deposit Insurance Corporation ("FDIC"), the Office of Thrift Supervision ("OTS"), the Office of the Comptroller of the Currency ("OCC"), and the Board of Governors of the Federal Reserve System ("FED") issued interagency guidelines ("Interagency Guidance"), pursuant to authority granted by GLB, that proposed that notices be issued whenever it is reasonable to expect that sensitize personal information will be "misused" in an manner that creates "substantial harm or inconvenience" to the consumer. We believe it is essential for Congress to articulate the broad parameters of what regulators should consider when providing guidance to the industries under their supervision, and we would prefer that that standard parallel the one endorsed by FTC Chairwoman Deborah Majoras in testimony she delivered last June before the Senate Commerce Committee. She suggested a standard for notification that ties a breach to a "significant risk of identity theft". As she observed when she testified, "It is important to note...that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." We would add that they can also happen – and be caught by the victim of the breach – before any risk of any kind affects consumers.

The Coalition recognizes that HR 3997 has embraced language tracking the OCC guidance as the trigger for notification, but it has also performed a public service by trying to define the term in section 630(k)(11) in the way it has. We also hope that the Securities and Exchange Commission ("SEC"), like the Interagency Guidance, will act as soon as practicable to follow the example of the other functional regulators and provide interim guidance for businesses that they supervise.

4. **Reasonable Compliance Obligation.** Breach security and notification are complicated matters, and how security is defined and implemented is equally technical. We believe that the functional regulators of the affected industries, including the FTC for those businesses not currently subject to functional regulation, are best suited to supervise and enforce the decisions Congress makes in this arena. Only they can adequately evaluate the risks to consumers served by the whole range of businesses that have custody over sensitive personal information pertaining to them. Only they can adequately track evolving technology, and adjust quickly and over time to effectively translate changes in that environment into regulations that are both reasonable and consistent with the law enacted by the Congress. Our members applaud the language in H.R. 3997, in proposed new section 630(i) of the FCRA, that attempts to encourage functional regulators to "jointly" develop regulations and to reconcile any differences by a date certain. The decision the bill makes, in proposed

subsection (j), to delegate exclusive enforcement authority to functional regulators is, in our judgment, a wise and prudent decision.

### **Conclusion**

In summary, the National Business Coalition on E-Commerce and Privacy supports the House Financial Services Committee's approach to this very important problem, as embodied in the legislative language of H.R. 3997. As we have said from the inception of this debate, it is critical to approach the problem of data security and notification in a responsible and thoughtful manner, keeping in mind the need to narrowly tailor legislation that embraces the principles which the Coalition has articulated above. We are pleased that most of the bills now under consideration have been drafted, to one degree or another, with these principles in mind.

As we have also tried to demonstrate in this statement, it is equally important that during the course of its consideration of H.R. 3997, the Committee resist the temptation to expand the coverage of this legislation to include subjects unrelated to data security and notification, such as efforts to require (for privacy reasons) consumer rights to access and correct data held by businesses, regardless of any breach of security. As H.R. 3997 evidences, the issues of data security and breach notification involve the security of sensitive personal information from unauthorized access by illegal activity or negligent behavior, while data privacy involves the regulation of lawful sharing of such data by businesses that legally acquire and safeguard it. The two issues should be addressed separately, as acknowledged by the current framework of H.R. 3997.

On behalf of the Coalition, we look forward to the opportunity to continue to work with the Members of this Subcommittee and the full Committee, and their staffs, as this legislative process proceeds.