Consumers Union
Nonprofit Publisher of Consumer Reports

U.S. Public Interest Research Group

Consumer @ction

Center For Democracy & Technology

CFA Consumer Federation of America

Privacy Rights Clearinghouse

21 July 2006

Re: Do not bring H.R. 3997, the Financial Services Data "Security" Bill, to the Floor

The Honorable Dennis Hastert
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

The Honorable Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, DC 20515

The Honorable John Boehner
Majority Leader
U.S. House of Representatives
Washington, DC 20515

The Honorable Steny Hoyer
Minority Whip
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Speaker, Representatives Boehner, Pelosi, and Hoyer:

Consumers Union, the nonprofit, independent publisher of *Consumer Reports,* the U.S. Public Interest Research Group, the Consumer Federation of America, the Center for Democracy and Technology, Consumer Action, and the Privacy Rights Clearinghouse understand that the House leadership plans to schedule a floor vote for next week on H.R. 3997, the "Financial Data Protection Act." We strongly oppose this controversial legislation and urge you instead to bring to the floor H.R. 4127, the "Data Accountability and Trust Act," a much more consumer-friendly bill that was unanimously passed by the Energy & Commerce Committee.

As highlighted by the more than 100 security breaches involving nearly 90 million Americans since the ChoicePoint fiasco in February 2005, consumers can do everything right to keep their financial well-being in order and still be at risk for identity theft through no fault of their own. Unfortunately, H.R. 3997 moves us in the exact wrong direction.

Individuals need to be notified when their sensitive personal information has been breached, so they can take reasonable steps to avoid becoming victims of identity theft (e.g., placing security freezes and fraud alerts on their credit files, carefully checking their credit reports, reviewing their financial statements, etc.). In addition, when companies are required to notify individuals of data breaches, those companies have a market-based incentive to put in place strong security procedures to avoid breaches in the first place.

Today, we enjoy a *de facto* national standard in which companies notify individuals nationally based on the strongest state laws when their personal information has been lost or stolen. H.R. 3997 overturns existing state notice of breach laws and weakens this *de facto* national standard. It requires individual notification only after the company experiencing the breach decides that the breach is "reasonably likely" to result in actual ID theft or account fraud. We call this a "don't know, don't tell" policy because if a company doesn't know whether consumers will be victimized, it does not have to notify them. H.R. 3997 even allows regulators to permit a company to consider the monitoring software it has in place after a breach as a reason not to tell consumers that their debit card numbers and corresponding PINs have been stolen. Further, H.R. 3997 does not apply to every type of company that holds sensitive data such as Social Security numbers. Its definition of "covered entity" is also much more limited than current state notice of breach laws.

H.R. 4127 is a much better model for any federal notice requirement. It requires companies to notify individuals of a breach involving sensitive personal information unless the company can show that there is no reasonable risk of harm. In this case, if companies cannot determine whether there is a reasonable risk of harm, then they would still have to notify individuals. This avoids the "don't know, don't tell" approach to notification.

H.R. 3997 and H.R. 4127 also each contain provisions on safeguarding personal information, but H.R. 3997 would use those provisions to stop progress toward data protections by states. H.R. 3997 would preempt a broad array of state laws addressing the responsibility to protect the security or confidentiality of information on consumers and to safeguard such information, with the preemption going well beyond the limited protections provided by the bill. H.R. 4127, by contrast, limits its preemption only to state laws that address information security practices similar to those required under the federal bill.

Another important difference in the bills is that H.R. 3997 only rolls back existing state laws and does not provide any new rights, while H.R. 4127 gives consumers the new right to review and dispute information held by data brokers like ChoicePoint, which are unregulated when they act in areas outside of the Fair Credit Reporting Act (FCRA). Data brokers gather and sell personal information on almost all Americans in the form of detailed dossiers that, as we know from regular news reports, are vulnerable to security breaches.

In the wake of ChoicePoint and the myriad other data breaches in the past two years, the House leadership should work to bring to the floor a bill that provides real identity theft protections for consumers. It certainly should not bring to the floor a bill that does nothing positive for consumers and rolls back existing state consumer protection laws. We urge the House to vote on H.R. 4127, rather than H.R. 3997, a bill that would actually reduce the security of our personal information and could lead to greater instances of identity theft.

Thank you for your time and consideration. If you have any questions, please do not hesitate to contact Susanna Montezemolo at (202) 462-6262.

Sincerely,

Susanna Montezemolo
Policy Analyst
Consumers Union

Ed Mierzwinski
Director of Consumer Programs
U.S. Public Interest Research Group

David Sohn
Staff Counsel
Center for Democracy and Technology

Travis Plunkett
Legislative Director
Consumer Federation of America

Linda Sherry
Director of National Priorities
Consumer Action

Beth Givens
Director
Privacy Rights Clearinghouse

cc: Members, U.S. House of Representatives