



3 May 2007

The Honorable Patrick Leahy, Chairman
The Honorable Arlan Specter, Ranking Member
U.S. Senate Committee on the Judiciary
Washington, DC 20510

**RE: S. 495, Leahy/Specter "Personal Data Privacy and Security Act of 2007"
OPPOSE SESSIONS AND OTHER WEAKENING AMENDMENTS**

Dear Chairman Leahy, Senator Specter and Members of the Committee:

We are writing on behalf of the one million members of the non-profit, non-partisan state Public Interest Research Groups (PIRGs) to offer our views on S. 495, The Personal Data Privacy and Security Act of 2007.

While we commend the committee's leadership for including important provisions in this data security bill, such as its title holding largely unregulated data brokers accountable to consumers under most of the Fair Information Practices, we cannot support the underlying bill for three reasons we detail below. For similar reasons, although its provisions are not exactly the same, we cannot support S. 239, the Notification of Risk to Personal Data Act of 2007 (Feinstein).

Yet, we also strongly oppose further weakening amendments, such as an anticipated Sessions amendment that could (1) insert a "don't know, don't tell" trigger test before breach notification, (2) expand further a financial fraud prevention safe harbor (that should instead be eliminated or at least narrowed to protect debit card victims of TJX-like breaches) and (3) broaden the bill's preemption of state laws even further.

Here are the three reasons we cannot support the underlying bill, S. 495: First, it unwisely would preempt the states from most actions to protect privacy in many areas covered by the bill, even though the states have demonstrated clear leadership on privacy and other matters. Increasingly, the Congress is acceding to the indefensible demands of regulated industries that the price of any federal regulation, no matter how modest, must be permanent restrictions on the state laboratories of democracy.

Second, while the bill generally requires companies to provide notice to consumers who are victims of breaches, it allows companies to avoid notice upon a finding of "no significant risk." This **exception** standard, while better than the trigger standard in the Sessions bill (which does not require notice until and only if significant risk is first **affirmatively** shown), is weaker than the best state laws and would also preempt them all. The word "significant" should be deleted.

Third, the bill includes another exception to notice whenever companies are part of fraud prevention programs, even though these programs may not prevent all the money in a consumer's checking account from being vacuumed out by a thief. Ideally, this section should be eliminated. If not, at the very least, such a safe harbor should be limited to situations involving credit cards, but not debit cards, which directly access customer savings, checking and other accounts. **It is possible that were your language in effect, it might have immunized TJX (TJ Maxx and Marshalls) from notification in its recent 45 million credit and debit card number breach. The Sessions language is even broader and more unacceptable.**

Consumers are largely unaware of the risks of debit cards, and are primarily protected only by contractual promise, not by law. While credit cards are protected by the strong terms of the Truth In Lending Act, debit cards (which look the same but access your own accounts) are subject to the weak Electronic Fund Transfer Act, which allows banks unduly long investigation periods before reinstating money into a victim's account and, under some circumstances, even allows the bank to deny all the consumer's restitution claims even after fraudulent activity. Conversely, the Truth In Lending Act limits a consumer's fraud liability to \$50, by law.

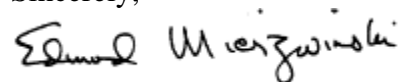
Federal law already leaves debit-card consumers less protected than they should be; your bill should not increase their risks by granting a safe harbor from notification when breaches could result in fraud and consumers could lose all the money from their accounts, then be forced to rely on unacceptably weak existing legislation (EFTA) to try to get their own money back.

On the matter of state preemption, we believe strongly that federal law should always serve as a floor, not a ceiling. States have demonstrated an ability to respond more quickly to privacy and other problems, including global warming. On the matter of privacy alone, seven states (led by Vermont) gave consumers the right to a free credit report before Congress acted, forty states had do-not-call lists before the FTC acted, at least three-dozen states have security breach notification laws (and this bill is weaker than an estimated 23 of them yet would preempt them all), and some twenty-eight states have given consumers the right to prevent identity theft through placement of a security freeze on their credit reports.

Industry claims to the contrary, the states never enact 50 different laws; indeed they tend to enact a few similar laws and then other states perfect those efforts with virtually identical laws. When Congress steps in, it should create a federal floor protecting consumers in the few remaining unprotected states; it should not override the stronger state laws, nor should it prevent further experimentation. Any specious industry claims of compliance costs could be met by simply complying with the strongest state law nationwide, as many firms have done following the first widely-reported breaches.

We look forward to working with the committee to enact a final federal privacy law that holds industry accountable to protect our sensitive information, protects consumers and protects the right of the states. Please have your staff contact me at edm@pirg.org or 202-546-9707 if they have any questions.

Sincerely,



Edmund Mierzewski
Consumer Program Director