Members
House Financial Services Committee
2129 Rayburn HOB
Washington, DC 20515

12 September 2018

Via email

OPPOSE HR6743, The Consumer Information Notification Requirement Act (Luetkemeyer)

Dear Representative:

We write as leading state and national consumer, civil rights, civil liberties and privacy organizations to oppose HR6743, the Consumer Information Notification Requirement Act, to be considered in committee this week. The preemptive bill might also be called the "Equifax Protection Act."

The bill is unnecessary, since it (Section 2) largely restates and even narrows the modest breach notice requirements of the privacy rules prepared by the prudential regulators and the Federal Trade Commission in response to the 1999 Gramm-Leach-Bliley Act. You may recall that while the GLBA was passed largely to enable mergers between banks, securities firms and insurance companies (to create one-stop "financial supermarkets"), its Title V was included to address a number of privacy violations and data sharing abuses at the time by regulated firms.

The bill shackles its modest re-shuffling of existing agency breach response rules for financial institutions to the preemption of all state data breach, data security and other privacy laws (Section 3), as they apply to both "financial institutions and their affiliates." "Financial institution" is a term that includes numerous non-banks including Equifax and the other consumer reporting agencies, as well as debt collectors and payday lenders. This is unacceptable.

All states already require data breach notices, many in any circumstance where information might be compromised (acquisition standard). But both the current GLBA scheme under regulatory rules and HR6743 limit breach notices only until after the breached entity itself determines that the breach is "reasonably likely" (a "trigger") to result in a "harm," here defined narrowly to mean only "identity theft, fraud or economic loss." This "harm trigger," coupled with a narrow harm definition, throws out many state laws that recognize that data breaches can have other negative impacts on the victims and force companies to do a better job protecting information by requiring notice whenever it is compromised. Further, the HR6743 scheme is much more restrictive of state protections than the current federal agency rules, since it narrows the definition of harms requiring notice described in those rules while its preemption scope is expanded from GLBA rules concerning only "nonpublic personal information" to instead now cover any state laws concerning securing **any** personal information."

Harm triggers only increase the chance that you won't be notified of hacks, because many of these hacks won't fit within the law's definition of harm. Harm triggers also diminish a

company's incentive to improve its data security practices because it can get out of having to let customers know about certain breaches.

There are many non-financial harms that can result from a data breach, such as harm to dignity from the compromise of nude photos, or harm to reputation from the compromise of personal email. A breach could even lead to physical harm, such as if logs of a domestic violence victim's calls to a support hotline were to fall into the wrong hands. By weakening the notice standard in the overwhelming majority of states, this law would cause consumers to stop receiving notifications about breaches that they currently have a right to hear about today— breaches that could lead to physical or emotional harm.

Many states are innovating in these areas and also protecting more forms of information – not simply financial – from misuse. For example, several states have established biometric privacy and medical information privacy laws; others have protected log-in credentials for online accounts and electronic signatures. Further, states could more quickly respond to new or emerging harm threats than Congress, as they have numerous times in the past, if they are not preempted.

The bill is made much more dangerous, however, by the broad scope of Section 3, which replaces a narrow preemption provision in the existing GLBA with a sweeping provision that could not only eliminate all state data breach notice, data security and other privacy laws as they apply to financial institutions as broadly defined, but forestall further state innovation to protect their citizens from future privacy, data security threats. Further, the addition of "and affiliates" to the preemption language appears intended to further broaden the scope of firms covered by the bill absent hearings or review of its implications.

Finally, it is particularly inappropriate that just one year after the massive Equifax data breach, resulting from the failure of a company supposedly covered by the FTC's existing GLBA Safeguards Rule to maintain data security over a treasure trove of financial DNA, that the committee is considering weakening data security and data breach laws, instead of strengthening them or passing legislation to make companies like Equifax more accountable to their victims.

Please contact Ed Mierzwinski of U.S. PIRG at edm<at>pirg.org if you or your staff have any questions.

Sincerely,

Access Humboldt
Allied Progress
American Civil Liberties Union
Americans for Financial Reform
Campaign for a Commercial-Free Childhood

Center for Digital Democracy
Common Sense Kids Action
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Digital Privacy Alliance
Electronic Frontier Foundation
Media Alliance
NAACP
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low-income clients)
National Consumers League
National Network to End Domestic Violence
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
Public Citizen
Public Knowledge
Reinvestment Partners
U.S. PIRG
World Privacy Forum