



November 8, 2017

The Honorable John Thune  
Chairman, Committee on Commerce,  
Science, and Transportation  
United States Senate  
Washington, DC 20510

The Honorable Bill Nelson  
Ranking Member, Committee on Commerce  
Science, and Transportation  
United States Senate  
Washington, DC 20510

RE: Hearing on Protecting Consumers in the Era of Major Data Breaches

Dear Chairman Thune and Ranking Member Nelson:

The National Retail Federation applauds your holding of today's hearing to review the recent breaches of data security at Equifax and Yahoo that have collectively affected billions of consumers globally, and hundreds of millions of American citizens. Consumers in the United States did not receive clear and timely notice of these breaches and, in the case of Yahoo, did not learn of some of their recently reported breaches for years. Similarly, financial institutions and third-party service providers have sought to maintain exemptions in breach legislation that permit them to keep the fact of their own breaches secret. For over a decade, NRF has supported, and worked with members of this Committee to craft, federal data security legislation that would create a uniform, national requirement for *all* breached businesses to provide notice of their breaches to affected individuals.

By way of background, NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

According to the [2017 Verizon Data Breach Investigations Report](#), all sectors of U.S. industry are affected by security breaches, but three collectively account for the majority of all breaches, defined as security incidents with confirmed data loss. Verizon reported that the financial services sector had 24.3% of all breaches last year, while the healthcare sector accounted for 15.3% and the public sector (e.g., governmental entities) had 12.4%. Not surprisingly, these sectors also handle American's most sensitive personal information, and the hackers know this. By contrast, businesses with less sensitive data generally account for fewer breaches. Verizon reported, for instance, that the retail industry suffered just 4.8% of all breaches last year. The bottom line is that all entities that handle consumers' personal information, whether they do so through direct contact with customers or as third parties, face security threats that put at risk any sensitive data in their possession. To protect customers comprehensively, federal laws must apply to *all* sectors and leave no holes for some industries that hackers can exploit.

Some federal breach bills under consideration contain “notice holes” – exemptions from the legislation’s breach notice provisions altogether, or special provisions that permit some types of businesses to shift their breach notice obligations onto others. The companies testifying today would enjoy exemptions in leading House breach legislation under both scenarios. For example, under the breach legislation reported by the House Financial Services Committee last Congress, Equifax is exempt from the bill’s provisions, as are banks, credit unions and other entities that qualify as “financial institutions” under the Gramm Leach Bliley Act (GLBA). Enacted in 1999, however, GLBA *predates* the first state breach notification law by four years, and consequently it contains no statutory requirement for breached financial institutions to notify affected individuals of their breaches. Furthermore, the regulatory guidance issued under GLBA merely states that financial institutions “should” notify affected individuals following a breach, not “must.” Not surprisingly, banks, credit unions and the broader financial services sector only support federal breach legislation that would preserve this notice hole by exempting GLBA-covered entities from any requirements to notify consumers affected by a breach.

Under the second scenario, special breach notice provisions would actually *permit* these breached businesses to shift the obligation to notify affected consumers of their own breach onto the unbreached businesses they serve. Verizon, for instance, only supports breach legislation where it qualifies as a “service provider” and enjoys special notice exemptions, such as in the bills reported by both the House Financial Services Committee and House Energy & Commerce Committee. Under these bills, qualifying service providers are *not* required to make notice of their *own* breaches. In some circumstances under these bills, they can even be aware of a breach of their own network and not be required to make notice of the breach to anyone at all – not to affected consumers, not to affected businesses, and not to government enforcement authorities. In other circumstances, qualifying service providers can simply shift the obligation to notify affected consumers onto the businesses they serve. This special treatment, which amounts to a notice hole for ISPs, is unjustified, particularly when consumers are affected by breaches wherever they occur.

As this Committee considers federal breach legislation in the wake of the Equifax and Yahoo breaches, we urge you to avoid the flaws in previous attempts at federal legislation by closing the notice holes that would permit financial institutions and service providers to avoid making notice of their breaches. We look forward to working with you and the members of the Committee to enact federal data breach legislation that establishes a uniform breach notification standard so that all Americans will be notified by businesses that have suffered a breach of security affecting their sensitive personal information.

Sincerely,



David French  
Senior Vice President  
Government Relations

cc: The Honorable Mitch McConnell  
The Honorable Chuck Schumer  
Members of the Senate Commerce Committee