December 4, 2019

The Honorable Roger Wicker
Chairman
U.S. Senate Committee on Commerce,
Science and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on Commerce,
Science and Transportation
511 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell,

The National Multifamily Housing Council (NMHC) and National Apartment Association (NAA) applaud the Committee for examining legislative solutions to bolster consumer privacy and exploring a variety of issues surrounding the collection, use and protection of sensitive consumer information by private companies, such as apartment firms. Rental housing owners and operators, and their third-party service providers, rely heavily on highly sensitive, personal data about apartment applicants, residents and employees to run their day-to-day business and, therefore, are actively engaged in these issues.

For more than 20 years, NMHC and NAA have partnered on behalf of America's apartment industry. Drawing on the knowledge and policy expertise of staff in Washington, D.C., as well as the advocacy power of more than 160 NAA state and local affiliated associations, NAA and NMHC provide a single voice for developers, owners and operators of multifamily rental housing. One-third of all Americans rent their housing, and 39 million of them live in an apartment home.

Given the amount of sensitive, personal and financial information that apartment operators rely on and the ever-expanding cyber-threat landscape we face, our industry has placed a high priority on strengthening our defenses against vulnerabilities and protecting sensitive data and consumer privacy. In fact, apartment firms are committing tremendous resources to this cause and NMHC and NAA work continually to educate firms about best practices in this space and how best to comply with emerging regulatory trends.

As the Committee considers solutions to bolster consumer and data protection in the wake of continued high-profile data security and privacy breaches, NMHC and NAA would like to use this as an opportunity to express support for federal legislation that would provide for:

- A clear federal preemption of the existing patchwork of often conflicting and contradictory state data security, privacy and breach notification laws. As we near implementation of the California Consumer Privacy Act (CCPA) and with several other

state laws being considered or enacted in recent months, the need for a strong, federal privacy and security standard is clear. Allowing governing bodies across the United States, or even across the globe, to create an uneven patchwork of regulation for data protection and privacy increases the compliance costs and regulatory burdens on American businesses of all sizes while leaving consumers vulnerable to a myriad of mistakes and unintended consequences.

- A flexible and scalable national standard for data security, privacy and breach notification. Specifically, when establishing compliance obligations, this standard must consider the needs and available resources of small businesses as well as large firms and the sensitivity of the data in question.

- A reasonable process by which consumers can control the data that is collected, accessed and utilized by businesses while ensuring that apartment firms maintain the right to collect, use and retain sensitive information that is necessary for day-to-day business operations such as resident screening and to comply with legal recordkeeping and regulatory requirements such as reporting under the Fair Housing Act.

- An obligation for third parties to maintain responsibility for their own security and privacy safeguards. Efforts to shift responsibility for third-party security lapses or privacy violations to apartment firms or other primary consumer relationship holders should be resisted. Often, businesses of all sizes are faced with the reality of being forced to accept boiler-plate contractual language in exchange for third party services. For example, while one company may have the market share and financial leverage to negotiate and demand certain security protocols, the vast majority of American businesses do not. The responsibility for overseeing a third party's data security program and consumer privacy safeguards should remain with the third party and not with apartment companies or other firms that rely on these third-party services.

- A clear assignment of financial and legal liability to the entity that actually suffered the data breach or caused the consumer privacy violation, particularly in the case of third-party breaches or security incidents.

- A requirement that third-party service providers first notify their customers of any breach and allow them the option to notify the consumer of the breach or privacy violation if they so choose. Ultimately, the reputational risk of a data breach or a failure to safeguard a renter's privacy falls to the apartment firm. For that reason, apartment operators should maintain control over communication with their residents. NMHC and NAA encourage apartment operators to ensure that service-provider contracts include strong and specific language governing data security, incident response and breach notification. Unfortunately, this can often be a significant challenge, especially for smaller property owners. For this reason, the law should be clear on this point.

We thank you for the opportunity to present the views of the rental housing industry as you continue deliberations to enhance consumer privacy and data security standards. NMHC and NAA stand ready to work with Congress to create a federal data, privacy and breach notification standard that recognizes the unique nature and needs of the rental housing industry while ensuring the data that our members collect, use and maintain is secure.

Sincerely,

Douglas M. Bibby
President
National Multifamily Housing Council

Robert Pinnegar
President & CEO
National Apartment Association