



May 8, 2024

The Honorable John Hickenlooper  
Chair  
Subcommittee on Consumer Protection,  
Product Safety and Data Security  
374 Russell Senate Office Building  
Washington, DC 20510

The Honorable Marsha Blackburn  
Ranking Member  
Subcommittee on Consumer Protection,  
Product Safety and Data Security  
357 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chair Hickenlooper and Ranking Member Blackburn:

On behalf of the members of the National Multifamily Housing Council (NMHC) and the National Apartment Association (NAA)<sup>1</sup>, we applaud the bipartisan, bicameral work being done to establish a long-overdue federal data privacy standard that protects consumers and American businesses, including apartment firms. As the Subcommittee on Consumer Protection, Product Safety and Data Security builds upon these conversations, NMHC and NAA wish to thank you for the leadership on these critical issues.

Apartment owners and operators, and their service providers, rely heavily on highly sensitive, personal data about apartment applicants, residents and employees to run their day-to-day business. Therefore, they are actively engaged in these issues. Given the sensitivity of the information that apartment operators rely on and the ever-expanding cyber threat landscape we face, our industry has placed a high priority on strengthening defenses against vulnerabilities and protecting sensitive data and consumer privacy. In fact, apartment firms are committing tremendous resources to this cause.

As the Subcommittee discusses the need for a national privacy standard and the ways in which federal legislation, like the recently released bipartisan and bicameral American Privacy Rights Act (APRA) would better protect consumers, NMHC and NAA would like to share our perspective. Outlined below are NMHC and NAA's priorities in this space, many of which are included as part of ARPA. We believe that these priorities should serve as a starting point for any federal data privacy and security measure:

- **Federal Preemption:** APRA outlines a federal preemption for most existing state data privacy and security laws. NMHC and NAA believe a clear federal preemption is necessary to provide clarity for apartment firms. The current patchwork of state laws

---

<sup>1</sup> For more than 25 years, the National Multifamily Housing Council (NMHC) and the National Apartment Association (NAA) have partnered to provide a single voice for America's apartment industry. Our combined memberships are engaged in all aspects of the apartment industry, including ownership, development, management, finance and suppliers partners/service providers. NMHC represents the principal officers of over 1,500 firms that own, develop, manage and finance apartments. As a federation of more than 145 state and local affiliates, NAA encompasses over 95,000 members, 141 affiliates, and more than 11.6 million apartment homes globally. The apartment industry today plays a critical role in housing this nation's households by providing apartment homes to 40.1 million residents, contributing \$3.4 trillion annually to the economy while supporting 17.5 million jobs.

creates a significant compliance burden for apartment firms and leaves consumers vulnerable to a myriad of mistakes and unintended consequences. This is particularly true given the constantly evolving nature of state data privacy and security laws.

- **Flexible and Scalable National Standard:** APRA reflects a need to take into consideration the data collected and the size of the company. NMHC and NAA believe any enforcement regime must provide for a flexible and scalable national standard for data security, privacy and breach notification that takes into account the needs and available resources of small businesses, as well as large firms and the sensitivity of the data in question.
- **The Ability to Continue to Perform Essential Business Functions:** APRA encourages data collection minimization and also rightfully acknowledges that entities may have an essential business need to engage with consumer data. Apartment firms must maintain the right to collect, use and retain sensitive information necessary for business operations. This is particularly important to ensure the safety and security of apartment residents and employees through prospective resident screening while also ensuring compliance with regulatory requirements such as reporting under the Fair Housing Act.
- **Clarity in FTC's Role in Rulemaking and Enforcement:** APRA designates enforcement will be carried out by the FTC. Should the FTC take on the role as regulator of data privacy and security laws, the scope of their rulemaking and enforcement role should be clarified to allow for entities to have a reasonable amount of time to respond to FTC and consumer inquiries. Additionally, entities that must comply with new data privacy and security regulations stemming from this legislation will need education, flexibility and the right to cure when the FTC notifies the entity of a possible violation before any enforcement action is taken.
- **Reasonable Time Frame to Respond to Consumers:** APRA directs the Federal Trade Commission (FTC) to promulgate regulations for compliance by covered entities. Given the complexities of verifying any privacy or protection request and responding accurately, apartment firms need sufficient time to carry out any request, with the option for an extension if necessary.
- **Third-Party/Service Provider Responsibilities:** APRA makes an important distinction between covered entities, service providers and third parties. We believe that service providers must hold responsibility for their own security and privacy safeguards. Liability for any third-party/service provider security lapse or privacy violation must not shift to apartment firms or other primary consumer relationship holders. Often, businesses of all sizes are faced with the reality of being forced to accept boilerplate contractual language when contracting with a service provider or supplier. For example, while one large 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 party that is collecting, using and retaining sensitive information—not with apartment companies or other firms that rely on third party services.
- **Assignment of Financial and Legal Liability:** APRA establishes the need to differentiate between a covered entity, their service provider or a third-party data collector. We support 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. 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 apartment 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 protection standard that recognizes the unique nature and needs of the apartment industry while ensuring the data that our members collect, use and maintain is secure.

Sincerely,



Sharon Wilson Géno  
President  
National Multifamily Housing Council



Robert Pinnegar  
President & CEO  
National Apartment Association