

June 4, 2025

The Honorable Andy Barr
Chairman, House Financial Services
Subcommittee on Financial Institutions
2430 Rayburn House Office Building
Washington, DC 20515

The Honorable Bill Foster
Ranking Member, House Financial Services
Subcommittee on Financial Institutions
2366 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Barr and Ranking Member Foster:

On behalf of the Real Estate Technology and Transformation Center (RETTTC), the National Multifamily Housing Council (NMHC), the National Apartment Association (NAA), we write to thank you for convening today's hearing, *"Framework for the Future: Reviewing Data Privacy in Today's Financial System,"* and to share insight on the need of a long-overdue federal data privacy standard that protects consumers and American businesses, including rental housing firms and our technology partners.

Rental housing owners and operators, and their service providers, rely heavily on highly sensitive, personal data about rental applicants, residents and employees to run their day-to-day business. Given the sensitivity of the information that rental housing 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, rental housing firms are committing tremendous resources to this cause.

To improve housing affordability and benefit millions of renters, the rental housing industry has embraced Artificial Intelligence (AI) technology. AI and related technologies in rental housing have led to significant gains in meeting resident expectation and demand. But along with its immense promise, AI also transforms the cyber risk landscape for the industry and brings a host of challenges. Cybercriminals are deploying this technology to execute more advanced attacks on businesses of all types. And the rental housing industry is no exception.

This evolving threat landscape makes the Subcommittee's hearing even more pressing. To effectively regulate AI and emerging technologies used by the rental housing industry and beyond, RETTTC, NMHC and NAA strongly believe that it is necessary to first establish a federal data privacy standard. As the subcommittee considers data privacy's role in our financial system, RETTTC, NMHC and NAA would like to take the opportunity to highlight our priorities in this space. We believe that these priorities should serve as a starting point for any other federal data privacy and security measure:

- **Federal Preemption:** A clear federal preemption is necessary to provide clarity for rental housing firms and their technology partners. The current patchwork of state laws creates a significant compliance burden for rental housing firms and leaves consumers vulnerable to mistakes and unintended consequences. This is particularly true given the constantly evolving nature of state data privacy and security laws. As our organizations have consistently said in the past, a fragmented regulatory approach in

data management, security and technology risks stifling innovation and increasing compliance costs. This ultimately undermines the benefits these systems and technologies offer to renters and housing providers alike.

- **Flexible and Scalable National Standard:** A data privacy and protection standard will benefit from taking into consideration the data collected and the size of the company. RETTC, NMHC, and NAA believe that 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:** Entities may have an essential business need to engage with consumer data and should be mindful of data minimization. Rental housing 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 residents and employees through prospective resident screening while also ensuring compliance with regulatory requirements such as reporting under the Fair Housing Act.
- **Reasonable Time Frame to Respond to Consumers:** Any data privacy and protection enforcement should provide for adequate time for rental housing firms to respond to inquiries. Given the complexities of verifying any privacy or protection request and responding accurately, rental housing firms need sufficient time to carry out any request, with the option for an extension if necessary.
- **Third Party/Assignment of Financial and Legal Liability:** There is 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 rental housing 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 rental housing companies or other firms that rely on third-party services.
- **Clarity in Regulatory Authority:** To provide clarity and certainty to apartment firms, a single federal agency should be responsible for data privacy and protection rulemaking and enforcement. Further, Congress should establish the scope of any federal regulator's authority. Entities that must comply with new data privacy and security regulations will need education, flexibility and the right to cure in the event of a possible violation.
- **Preserving Innovation:** As policymakers seek to determine how to best regulate AI and other emerging technologies, they should be cautious not to stifle innovation or inhibit the development of tech-driven, pro-consumer solutions. That said, it is also imperative for Congress to protect consumers, businesses, and national security from the growing threat of cybercrime. The most effective way to achieve both of these goals

is through focusing on the development of a robust, flexible, and scalable federal data security and privacy standard.

We appreciate the Subcommittee's leadership in enhancing consumer privacy and data security standards within our country's financial system. RETTC, 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 rental housing industry while ensuring the data that our members collect, use and maintain is secure.

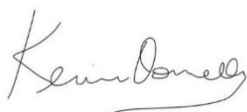
Sincerely,



Sharon Wilson Géo
President
National Multifamily Housing Council



Bob Pinnegar
President and Chief Executive Officer
National Apartment Association



Kevin Donnelly
Executive Director and Chief Advocacy Officer
Real Estate Technology & Transformation Center