March 16, 2026

The Honorable French Hill
Chairman
House Financial Services Committee
1533 Longworth House Office Building
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
House Financial Services Committee
2221 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Hill and Ranking Member Waters:

On behalf of the members of the National Multifamily Housing Council (NMHC), the National Apartment Association (NAA), and the Real Estate Technology and Transformation Center (RETTC), thank you for convening the hearing entitled "Updating America's Financial Privacy Framework for the 21st Century." We write to share insights on the need for a long-overdue federal data privacy standard that protects consumers and American businesses, including rental housing firms and our technology partners.

Data Sensitivity in Rental Housing

The relationship between a resident and housing providers may span years and involve the collection and use of various types of information. Consumer data contained in resident screening reports and held by housing operators and their service providers helps document rental history, tenure, and payment data, which are key components of a resident's profile. These data points can also help expand a resident's housing opportunities in the future.

Rental housing owners and operators, and their service providers, rely heavily on sensitive personal data about rental applicants, residents, and employees to run their day-to-day business and effectively integrate new technologies into their operations. Given the sensitivity of the information on which rental housing operators rely, and the ever-expanding cyber threat landscape, rental housing has placed a high priority on strengthening defenses against vulnerabilities and protecting sensitive data and consumer privacy.

Need for a National Data Privacy and Security Standard

As privacy legislation is further developed, policymakers can ensure American competitiveness by prioritizing innovation. Federal, state, and local policies should preserve the ability of housing providers to use AI and other emerging technologies, enabling better and more affordable housing for renters.

Excessive compliance costs stemming from conflicting state privacy regimes increase operational costs for housing providers, which can translate into higher housing costs for renters.

To effectively regulate AI and emerging technologies used by the rental housing industry and beyond, NMHC, NAA, and RETTC believe that it is essential to first establish a federal data privacy standard. Because AI systems rely on data inputs, establishing clear national standards for data privacy and

security should precede the imposition of new regulations governing AI development and deployment.

As the Committee considers data privacy's role in our financial system, NMHC, NAA, and RETTC thank you *for the* opportunity to highlight our priorities. We believe that these priorities should serve as a starting point for any other federal data privacy and security measure.

Policy Principles

1. **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 significant compliance burdens for rental housing firms and increases the risk of inconsistent protections for consumers. This is particularly true given the constantly evolving nature of state data privacy and security laws.

   As our organizations have consistently said, 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.

2. **Flexible and Scalable National Standard**

   A data privacy and protection standard should account for the data collected and the size of the company.

   NMHC, NAA, and RETTC believe that any enforcement regime must provide a flexible and scalable national standard for data security, privacy, and breach notification that accounts for the needs and available resources of both small businesses and large firms, as well as the sensitivity of the data in question.

3. **The Ability to Perform Essential Business Functions**

   Rental housing firms must maintain the right to collect, use, and retain sensitive information necessary for business operations while remaining mindful of data minimization principles. 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.

   Enforcement should be carried out by federal regulators and state attorneys general to ensure consistent application of the law and avoid excessive litigation that could undermine innovation and housing affordability.

4. **Reasonable Time Frame to Respond to Consumers**

Any data privacy and protection enforcement should provide 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 such requests, with reasonable extensions when necessary.

5. Assignment of Financial and Legal Liability

There is an important distinction between covered entities, service providers, and third parties.

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.

Businesses of all sizes are often forced to accept boilerplate contractual language when contracting with service providers or suppliers. While large companies may have the market leverage to negotiate security protocols, most American businesses do not.

Responsibility for overseeing a third party's data security program and consumer privacy safeguards should remain with the entity collecting, using, and retaining sensitive information—not with the firms that rely on third-party services.

6. Enforcement and 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.

Congress should clearly define the scope of that regulator's authority. Entities subject to new privacy and security regulations will need education, flexibility, and the right to cure potential violations before enforcement penalties are imposed.

Any creation of a private right of action allowing consumers to sue companies for a privacy breach, while well-intended, could open the door to costly litigation that could negatively impact housing operations and ultimately housing affordability, even when the rental housing owner or operator has taken reasonable steps and has made a good faith effort *to* secure the privacy and data of its residents.

7. Safe Harbors and Good Faith Compliance

Congress should also consider safe harbor provisions for companies that implement recognized cybersecurity and privacy best practices in good faith. Safe harbor protections can encourage companies, including rental housing providers, to expand investment in robust data security programs and adopt widely used frameworks.

Providing reasonable protections for companies that demonstrate good-faith efforts to comply with the forthcoming federal privacy and security standards would promote stronger

cybersecurity practices while allowing businesses to focus resources on preventing breaches rather than responding to excessive litigation.

Artificial Intelligence and Innovation

NMHC, NAA, and RETTC believe it is essential first to establish a federal data privacy standard before considering expanded regulations of AI and emerging technologies.

As policymakers consider how to regulate AI and other emerging technologies, they should avoid approaches that stifle innovation or inhibit the development of pro-consumer solutions while also protecting consumers, businesses, and national security from cyber threats. Establishing a robust, flexible, and scalable federal data security and privacy framework is the most effective way to achieve both goals.

Rental housing providers are increasingly using technologies such as AI to improve operations, increase efficiency, and enhance housing affordability for millions of American renters. Today, AI-enabled technologies support leasing, fraud detection, maintenance systems, and resident services. As with many sectors, the rental housing industry seeks to leverage the benefits of these technologies while ensuring strong data protection and compliance with existing federal, state, and local laws, including the Fair Housing Act and the Fair Credit Reporting Act.

Conclusion

We appreciate the Committee's focus on enhancing consumer privacy and data security standards within our country's financial system. NMHC, NAA, and RETTC 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 our members collect, use, and maintain remains secure.

Sincerely,

Sharon Wilson Géno
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