December 6, 2019

(via email PrivacyRegulations@doj.ca.gov)

Attorney General Becerra
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: National Multifamily Housing Council Comments
Regarding the Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra:

The National Multifamily Housing Council ("NMHC") submits the following comments to the proposed California Consumer Privacy Act Regulations issued on October 10, 2019 ("Proposed Regulations").

INTRODUCTION

Based in Washington, D.C., NMHC is a national nonprofit association that represents the leadership of the apartment industry. Our members[1] include ownership, development, management, and finance entities who help create thriving communities by providing apartment homes for 40 million Americans. NMHC members own, develop, and manage apartment communities with more than five (5) units that range in product type from garden style communities to mid- and high-rise properties. NMHC members work to house Americans across all income levels by developing and managing properties that include affordable, student, senior, workforce, military, and luxury rental housing and contribute $3.4 trillion annually to the economy. In California, apartments and their residents contribute $499.1 billion to the state economy annually, supporting 2.1 million jobs. This includes $455.5 billion in local spending from California's residents. Almost 15 percent of the nation's entire apartment stock is located in the state of California. The following data underscores the apartment industry's importance in the U.S. consumer economy.

- 19.5 million U.S. households live in an apartment home (renter-occupied unit in a structure with five units or more). That is 44.6 percent of all renter-occupied households and 16.1 percent of all households.[2]

- Approximately 43.8 million U.S. households rent their housing (whether in an apartment home or single-family home). This is 36.1 percent of all households.[3]

[1] The comments made herein are attributed only to NMHC and not to any individual NMHC member.
[2] 2017 American Community Survey 1-Year Estimates, US Census Bureau, "Tenure by Units in Structure"
[3] 2017 American Community Survey, 1-Year Estimates, US Census Bureau "Tenure"

- Upwards of 108 million people, over one third of all Americans (34.0 percent),[4] live in rental homes (whether in an apartment home or single-family home).

INDUSTRY BACKGROUND

The multifamily industry faces booming demand for rental housing, which is being driven by a fundamental shift in our nation's housing dynamics as changing demographics and lifestyle preferences have driven more people away from the typical suburban house and toward the convenience of renting. This demand is fueled by a growing population, demand for rental housing by younger Americans, immigration trends, and Baby Boomers and "empty nesters" trading in single-family houses for apartments.

At the core of the industry is a focus on service to residents and a commitment to provide a safe and secure community for them to call home. That commitment extends to ensuring that information collected, used, or retained on apartment residents is secure and their privacy is safeguarded.

The lifecycle of consumer engagement in the apartment industry typically begins when an individual explores moving into a multifamily community. As the relationship between the renter and the apartment manager may span years, industry participants collect various types of information, some on a static basis, such as during initial resident screening in the leasing process, and some continuously, such as via rental and utilities payments or other interactions. The industry is somewhat unique in that its collection of information on consumers includes dynamic and non-traditional data types in order to provide quality housing to residents and enhance their living experience. Consumer data contained in screening reports and data generated regularly and held by property managers and their service providers is crucial in accounting for rental history, tenure, and payment data, which makes up an important part of a resident's profile and can serve as a tool to improve a resident's housing opportunities in the future. It is important to note for regulators and policymakers that the absence of such data could have unintended consequences for consumers.

The emergence and popularity of smart home and building technologies is changing how the multifamily industry designs and develops properties and how apartment firms are working to meet resident demand and expectation for new technologies and amenities. Given the inherent diversity in the nation's rental housing stock, deployment and management of these new technologies can vary significantly from property to property. For example, some rental housing providers offer a white-glove experience of several connected devices, ranging from smart thermostats to voice-activated devices, that are fully managed and maintained by the apartment firm. Others have chosen to offer these technologies as an amenity and instead give residents full control and management over these technologies, including connecting the devices to residents' own personal network.

In many cases, properties of all types are deploying smart building technologies that are revolutionizing operations and lowering the cost of providing housing. Apartment firms are

[4] 2017 American Community Survey, 1-Year Estimates, US Census Bureau "Total Population in Occupied Housing Units by Tenure"

implementing these devices to meet resident demand, increase the convenience of apartment living, and to create environmental and operational efficiencies. It is important to note that residents are demanding smart home technologies for many of these same reasons, including to improve the quality of their living experience, to reduce environmental impact, and to save money (*e.g.*, on utilities). The importance or desirability of smart home technology is only expected to increase in the future.[5] It is clear that resident preferences and the environmental, security, and financial benefits for both residents and apartment operators from these devices ensure that their deployment will continue to drive innovation in the multifamily industry.

The use of these devices in a multifamily context as opposed to use and deployment by an individual homeowner provides for unique security and privacy considerations that apartment firms take seriously. These technologies and the nature of the information exchanged create nuanced challenges and complexities for the industry in addressing the requirements in the Proposed Regulations. By way of example, the use of smart home technologies could result in the collection of certain data types that potentially could be considered personal information under the California Consumer Privacy Act ("CCPA"), but would differ significantly from traditional types of personal information, both in the type of information generated and the way in which it is transmitted and stored. Relatedly, certain data may be maintained in unstructured formats not conducive to being readily accessed or deleted.

These factors introduce unique complexities to the multifamily industry in complying with the Proposed Regulations as currently drafted. NMHC believes that the Proposed Regulations inadvertently create new risks to the privacy and security of consumer data. For example, the Proposed Regulations contemplate significant transmissions of personal information that would otherwise remain stored, which inherently creates privacy and security risks to consumers. NMHC believes many of these challenges can be addressed through clarifications and amendments to the Proposed Regulations. NMHC proposes that, to the extent possible, the California Government consider minimizing all scenarios where additional transmissions of personal information would be required in an effort to mitigate privacy and security risks to consumers. In addition to comments on specific sections set forth herein, NMHC believes the industry also would benefit from additional clarification and guidance in the Proposed Regulations around use cases that would constitute a "sale" of personal information as well as exceptions to deletion requests related to "internal uses," as contemplated by the CCPA.

As noted above, the privacy and security of consumers' information is of utmost importance to NMHC and its members. The comments set forth herein are intended to aid the Attorney General in further refining the CCPA regulations in an effort to better protect the privacy and security of consumers and streamline procedures to enable businesses' compliance with the law.

[5] According to the "2020 NMHC/Kingsley Renter Preferences Report," 44 percent of respondents indicated having five (5) or more Internet-connected devices and of those aged 18-34, half (50%) indicated having five (5) or more Internet-connected devices. Even further, 72.3% of respondents were interested in smart lighting; 66.8% interested in smart locks; 77.1% interested in smart thermostats, and 71.6% interested in a video doorbell. The report highlights survey results from 372,000 apartment residents nationwide, the largest ever in history, covering leasing decision factors, amenity desires, and the like. 2020 NMHC/Kingsley Resident Preferences Report, https://www.nmhc.org/research-insight/research-report/nmhc-kingsley-apartment-resident-preferences-report/.

COMMENTS REGARDING PROPOSED REGULATIONS

I. VERIFICATION PROCESS

The following sets forth NMHC's comments related to the verification requirements in Article 4 regarding (1) the general rules for verification; (2) the process for requests that cannot be verified; (3) the verification of requests made by authorized agents; and (4) privacy policy disclosures related to the verification process.

A. Verification of Requests – General Rules

The following sets forth NMHC's comments regarding the general rules for the verification process.

1. Proposed Regulations: Article 4, §§ 999.323-325

Article 4 of the Proposed Regulations requires businesses to establish, document, and comply with a "reasonable method" for verifying consumer requests; however, the Proposed Regulations offer little guidance as to what may constitute a "reasonable method."

2. NMHC Request and Recommendation

NMHC seeks further clarification as to "reasonable" verification methods. NMHC does not seek a prescriptive methodology for the verification process; rather, NMHC asks that the Proposed Regulations be amended to provide examples of verification methods that would be considered "reasonable" while permitting businesses to implement other methods at their discretion.

Further, NMHC recommends that the Proposed Regulations be amended to provide for a safe harbor from liability for businesses that follow a reasonable verification method.

3. Additional Analysis

As noted above, the Proposed Regulations do not provide specific guidance as to what would qualify as a "reasonable" verification method. Relatedly, as NMHC currently understands the Proposed Regulations, portions of Article 4 appear to be in conflict with other provisions of the Proposed Regulations. For example, section 999.323(b)(3)(a) instructs businesses to consider the sensitivity of personal information in implementing the verification process and that "[s]ensitive or valuable personal information shall warrant a more stringent verification process." However, section 999.313(c)(3) prohibits the disclosure of personal information that would create a substantial, articulable, and unreasonable risk. Section 999.323(b)(3)(a) also designates certain types of personal information as "presumptively sensitive," which are prohibited from disclosure pursuant to section 999.313(c)(4) (*e.g.*, Social Security number; driver's license number). The Proposed Regulations seem to suggest that businesses should implement stringent verification methods to disclose sensitive personal information (Section 999.323), while at the same time, the Proposed Regulations prohibit the disclosure of sensitive personal information (Section 999.313). Additional guidance on these topics would be beneficial to ensure compliance with the requirements and to protect the privacy and security of consumers.

NMHC believes this potential conflict can be rectified by amending the Proposed Regulations to (1) provide additional guidance as to what constitutes reasonable verification measures; and (2) eliminate the requirement that businesses provide specific pieces of personal information in response to access requests (as discussed in further detail in comments in section (II)(C) below).

B. Process for Requests that Cannot be Verified

The following sets forth NMHC's comments related to the process for requests that cannot be verified.

1. Proposed Regulations: Article 4, §§ 999.323-325

While Article 4 of the Proposed Regulations addresses, in part, a business's obligations when a request cannot be verified, NMHC believes further clarification is needed to protect consumers against fraudulent requests.

Relatedly, section 999.324(b) states that, if fraudulent or malicious activity is suspected, a business shall not comply with a request *until* the business can verify the request. NMHC is concerned that the current language implies a business is obligated to continually attempt to verify a request, without limitation, which could be unreasonable and unduly burdensome on businesses.

2. NMHC Request and Recommendation

NMHC seeks further clarification as to businesses' obligations where a request for access or deletion is denied because the consumer's identity cannot be verified through the verification process. Specifically, NMHC would like confirmation as to whether a consumer is entitled to attempt to rectify a request that was denied on verification grounds, and if so, what limitations may apply.

In addition, due to the security concerns presented by potential fraudulent requests or requests where a consumer's identity cannot be verified, NMHC recommends that the Proposed Regulations be amended to make clear that, where a business denies a request from a consumer on verification grounds, such consumer must wait 90 days, or some other additional period of time, before initiating another request, and the business is not obligated to respond to any requests purportedly received from that consumer before that time period is complete.

Finally, NMHC recommends the language in section 999.324(b) be amended as follows:

> ***999.324(b)***
>
> *(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete unless ~~until further~~ verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer. A business shall not be obligated to comply with a consumer's request to know or request to delete where the business has followed its verification procedures and is not able to verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.*

C. Verification of Requests – Authorized Agent

The following sets forth NMHC's comments related to the verification of requests made by authorized agents.

1. Proposed Regulations: § 999.326

Section 999.326 would permit an authorized agent to submit requests to know or requests to delete on behalf of a consumer. Without further direction as to verification requirements related to an authorized agent, NMHC believes the current proposed provision creates both privacy and security risks to consumers.

2. NMHC Request and Recommendation

NMHC recommends that the Proposed Regulations be amended to permit an authorized agent to act on behalf of a consumer only in the context of consumers' right to opt-out of the sale of their personal information and to require consumers to submit requests to know and requests to delete directly.

If the above change is not made, NMHC recommends in the alternative that the Proposed Regulations be amended: (1) to provide further guidance for verifying the identity and authority of authorized agents; (2) to permit businesses to confirm with a consumer directly that an authorized agent is authorized to act on their behalf; and (3) to provide a safe harbor from liability for businesses that follow the verification process.

Finally, NMHC proposes that the time period to respond to requests made by authorized agents be extended to 90 days and provide for an additional 90 day extension where necessary.

3. Additional Analysis

As noted above, NMHC believes allowing authorized agents to submit requests to know and requests to delete creates privacy and security risks to consumers. NMHC believes this risk is further heightened in the multifamily industry. As discussed above, apartment owners and managers collect various types of information on residents in order to operate and maintain apartment communities. The nature of this information differs substantially from, for example, information an online retailer may collect about its customers.

As a result, NMHC believes the risk of fraudulent authorized agent requests is not only higher in the multifamily industry, but also creates more serious risk to consumers than in other business contexts. For example, a nefarious actor could attempt to use the authorized agent process as a means to get sensitive information about residents, such as information pertaining to their living habits or lifestyle, all of which could present risk beyond identity theft—especially if the obligation to confirm specific personal information remains in the Proposed Regulations. In extreme cases, a bad actor who fraudulently obtained information about a resident could create physical security risks to consumers. NMHC member firms consider the safety and security of their residents to be of utmost importance and are concerned about the unintended consequences created by sharing sensitive data under the Proposed Regulations.

Further, given the importance of verifying that an authorized agent in fact has the authority to make requests on behalf of a consumer, the verification process for an authorized agent likely will require additional time than for consumers making requests directly. For example, a business may desire or need to obtain notarized documents, such as an affidavit, from both the agent and the consumer as part of the verification process to help protect against fraudulent requests. In the event the Proposed Regulations are not amended to limit authorized agent requests to only a consumer's opt-out right, increasing the time period to respond to requests made by authorized agents will further protect the privacy and security interests of all consumers.

D. Privacy Policy – Description of Verification Process

The following sets forth NMHC's comments regarding privacy policy disclosures related to the verification process.

1. Proposed Regulations: § 999.308(b)(1)(c)

Proposed Regulation section 999.308(b)(1)(c) requires that a privacy policy "[d]escribe the process the business will use to verify the consumer request, including any information the consumer must provide." While NMHC agrees that a verification process is necessary, NMHC believes the requirement to describe in detail the verification process, on a business's public website, potentially creates security risks to consumers that significantly outweigh any potential interest consumers may have in such information being publicly available in the business's privacy policy.

2. NMHC Request and Recommendation

To further protect consumers against fraudulent requests, NMHC proposes amending section 999.308(b)(1)(c) as follows:

999.308(b)(1)(c)

c. *Disclose that the business will require the consumer to verify their identity before the business may process the consumer request.* ~~*Describe the process the business will use to verify the consumer request, including any information the consumer must provide.*~~

In the event section 999.308(b)(1)(c) is not amended as set forth above, NMHC recommends in the alternative that the following requirement be omitted:

999.308(b)(1)(c)

c. *Describe the process the business will use to verify the consumer request*~~*, including any information the consumer must provide*~~.

3. Additional Analysis

Requiring businesses to make the verification process publicly available could serve as a roadmap for bad actors to institute fraudulent or nefarious access or deletion requests. While NMHC recognizes that bad actors may still seek to initiate access or deletion requests, and could ascertain the verification requirements through a business's request procedures, requiring the additional step of going through the submission process would mitigate this risk.

NMHC proposes that section 999.308(b)(1)(c) be amended to require only that businesses disclose in their privacy policy that consumer requests will be subject to a verification process. Doing so will put consumers on notice that verification requirements will apply to any request, and consumers will be informed of any verification procedures at the time a request is submitted.

II. REQUESTS TO KNOW AND REQUESTS TO DELETE

The following sets forth NMHC's comments regarding requests to know and requests to delete related to (1) methods for submitting requests; (2) the timeline for responding to requests; (3) responding to requests to know; and (4) responding to requests to delete.

A. Methods for Submitting Requests

The following sets forth NMHC's comments related to methods for submitting requests to know and delete.

1. Proposed Regulations: § 999.312

As NMHC currently understands the Proposed Regulations, Section 999.312 sets forth that businesses designate at least two methods for submitting requests to know and that at least one

method must reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods. NMHC believes this requirement is overly burdensome and does not serve the best interest of the consumer.

Section 999.312(a) further requires businesses that operate a website to use an "interactive webform accessible through the business's website or mobile application." NMHC believes that requiring use of webforms creates unnecessary security risk to consumers as webforms are often susceptible to security flaws and vulnerabilities.

2. NMHC Request and Recommendation

NMHC recommends that Section 999.312 be amended to permit businesses more flexibility in designating the request method in order to best serve the consumer. In particular, NMHC recommends that the section be modified to require businesses to offer the following two methods: (1) one method that reflects the primary method by which the business interacts with consumers; and (2) the second method be either a toll-free phone number or a method of submitting a request electronically.

Further, NMHC recommends that Section 999.312 be amended to omit the requirement for businesses to use a webform. Instead, NMHC proposes that Section 999.312 allow for businesses to designate a method for submitting requests electronically, which may include the creation of a basic user account, by the consumer or by the business on the consumer's behalf, for the sole purpose of implementing and completing the request process.

3. Additional Analysis

As noted above, NMHC believes consumers would benefit by permitting businesses additional flexibility in providing the method to submit consumer requests. For example, in the multifamily industry, a normal channel of communication often occurs in-person at the front desk or management office. In that case, a property management company may want to permit their residents to make requests in person (*e.g.*, via a tablet interface made available in the office, or via personnel who submit requests on residents' behalf) for the convenience of the resident. NMHC proposes that businesses be permitted to designate the method of submitting requests, which would include the primary communication channel with consumers as well as either a phone number or electronic submission.

In addition, NMHC is concerned that the requirement to offer a webform creates security risks to consumers. Due to their open interface, webforms are also prone to spamming and bot technologies, which could flood intake channels with illegitimate requests. While NMHC recognizes that CCPA section 1798.130(a)(2) prohibits businesses from requiring a consumer to create an account in order to make a verifiable consumer request, NMHC believes the privacy and security interests of the consumer are best served if businesses are permitted to require basic user accounts for the limited purpose of implementing the consumer request. Doing so will better allow businesses to verify the identity of the consumer and enhance security controls for the request process.

B. Timeline for Responding to Requests

The following sets forth NMHC's comments related to the timeline for responding to requests to know and to delete.

1. Proposed Regulations: § 999.313(b)

Section 999.313(b) of the Proposed Regulations states that the 45-day period for a business to respond to a request to know or delete "will begin on the day that the business receives the request, regardless of time required to verify the request." NMHC believes the current language creates unnecessary time constraints that may impair businesses' ability to conduct adequately its verification process and appropriately respond to consumer requests.

2. NMHC Request and Recommendation

NMHC recommends section 999.313(b) be amended as follows:

999.313

(b) Businesses shall respond to requests to know and requests to delete within 45 days. The 45- day period will begin on the day that the business verifies ~~receives~~ the request, pursuant to the verification requirements set forth in Article 4 ~~regardless of time required to verify the request~~. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is verified ~~received~~, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

If the above language is not accepted, NMHC proposes in the alternative the following amendments:

999.313

(b) Businesses shall respond to requests to know and requests to delete within 45 days. The 45- day period will begin on the day that the business receives ~~the~~ a complete request, regardless of time required to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the complete request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

999.301

"Complete request" means a request to know or request to delete where the consumer (1) has followed a business's designated method to submit the request and (2) submitted all required documentation and/or information required by the business as part of the designated submission process, including for the verification process.

3. Additional Analysis

NMHC believes the Proposed Regulations, due to the time restrictions, may reduce businesses' ability to take appropriate steps to verify adequately consumer requests. Requiring businesses to complete a verification process and to respond to requests in a specified time period, without flexibility, can result in inadvertent errors and incomplete procedures. For example, businesses may feel the need to rush or expedite the verification process in order to meet the 45-day timeline, which could result in inaccurate or insufficient verification procedures and increase the likelihood of both fraudulent requests and inaccurate or incomplete responses to requests. Consumers' privacy and security interests will be better served if the process encourages a thorough and thoughtful verification process that is not unnecessarily rushed due to regulatory time constraints. Amending the requirement so that the 45-day period begins once a business has verified a request will ensure that businesses have the opportunity to properly conduct the verification process and better protect consumers against fraudulent requests.

C. Responding to Requests to Know

The following sets forth NMHC's comments related to responding to requests to know.

1. Proposed Regulations: § 999.313(c)

Section 999.313(c) sets forth various requirements for responding to consumer requests that seek the disclosure of specific pieces of information about the consumer. NMHC believes the security risk presented by this requirement outweighs any interest the consumer may have in obtaining specific pieces of personal information from the business.

2. NMHC Request and Recommendation

NMHC recommends the Proposed Regulations be amended to require only that businesses respond to requests to know by disclosing categories and types of personal information collected on a particular consumer instead of specific pieces of personal information, including, but not limited to, by striking section 999.313(c)(1) in its entirety. Consumers will be better served by this approach because it will minimize security risks and streamline businesses' ability to respond appropriately to consumer requests.

3. Additional Analysis

Requiring businesses to disclose specific pieces of personal information increases the likelihood that such information could be misused or compromised. The Proposed Regulations appropriately recognize the inherent security risk in requiring businesses to provide specific pieces of personal information. For example, the Proposed Regulations expressly prohibit the disclosure of certain sensitive information (*e.g.*, Social Security numbers; driver's license numbers) as well as the disclosure of personal information that would create a "substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account…or the security of the business's systems or networks." *See* § 999.313(c)(3)-(4). The Proposed Regulations also require that businesses use "reasonable security measures" in the transmission of personal information to the consumer. *See* § 999.313(c)(6).

Rather than placing the burden on businesses to demonstrate in each case that providing certain personal information would create a substantial, articulable, and unreasonable risk, such risk can be eliminated through the regulations by requiring only that businesses disclose the categories and types of personal information. Doing so will not reduce or limit the consumer benefits of the CCPA as consumers will still have access to individualized categories and types of personal information that a business collects on them pursuant to Proposed Regulations section 999.313(c)(9)-(11).

In addition, requiring businesses to provide specific pieces of information creates inefficiencies in the response process as significant time would be required to identify and provide the individualized data for consumers. The requirement presents unique challenges to the multifamily industry, in particular, due to the nature of information collected, the business-to-consumer continuous relationship, and data collection between apartment residents and owners and managers, as well as the interdependencies of service providers who may collect residents' information. For example, providing specific information collected through smart home technology, to the extent the data would include CCPA personal information, would be impractical and potentially impossible, depending on the nature and format of the data. Alternatively, permitting businesses to instead disclose the general categories and types of information collected would be less burdensome for businesses and still appropriately inform the consumer as to what information is collected.

D. Responding to Requests to Delete

The following sets forth NMHC's comments related to responding to requests to delete.

1. Proposed Regulations: § 999.313(d)(3)

Section 999.313(d)(3) would permit a business to "delay compliance" with a request to delete where personal information is stored on archived or backup systems until the system is "next accessed or used." However, NMHC believes this requirement does not align with the functionality of many systems and practices.

2. NMHC Request and Recommendation

NMHC recommends that section 999.313(d)(3) be amended to provide for a complete exception to requests for deletion for personal information stored on archived or backup systems.

3. Additional Analysis

Data backups typically are not accessed on a regular basis and many are not in readily accessible formats. In the event a company needed to access backups, it is often indicative of an issue or failure with the primary systems. Moreover, the format and structure of data backups are not designed for the concept of deleting individual pieces of data (*e.g.*, backup tapes do not accommodate this function). The very purpose of a backup is to co-locate a copy of data so that it could be available to maintain business operations in the event the original data is corrupted, lost, or otherwise inaccessible. The reading of the Proposed Regulations would require a business to address an entire backup in full in order to delete specific personal information.

Doing so would create significant and unreasonable risk to the security and operation of the business, as all data on the backup would no longer be available.

III. REQUESTS TO ACCESS OR DELETE HOUSEHOLD INFORMATION

The following sets forth NMHC's comments related to requests to access or delete household information.

A. Aggregate Household Information

The following sets forth NMHC's comments related to requests for aggregate household information.

1. Proposed Regulations: § 999.318(a)

Section 999.318(a) of the Proposed Regulations would permit a consumer, without a password-protected account, to submit a request to know or request to delete as it pertains to household personal information and would obligate a business to respond by "providing aggregate household information." NMHC seeks further clarification as to this requirement.

2. NMHC Request and Recommendation

NMHC recommends that section 999.318(a) be stricken in its entirety. In the alternative, if section 999.318(a) is not deleted, NMHC seeks further clarification and guidance as to (1) what exact information businesses must provide in order to comply with the requirements, including clarification as to the definition of "aggregate household information"; and (2) the verification requirements to ensure all household members' privacy is adequately protected.

3. Additional Analysis

The term "aggregate household information" is not defined in the CCPA or the Proposed Regulations. "Aggregate consumer information," however, is defined as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, *that is not linked or reasonably linkable to any consumer or household*, including via a device." CCPA, § 1798.140(a) (emphasis added). If the intent of the Proposed Regulations is to permit individuals to access aggregate consumer information, as defined under the CCPA, doing so arguably goes beyond the requirements of the statute. Specifically, consumers' rights to request access or deletion are tied to the access or deletion of their personal information. Section 999.318(a), as proposed, seems to suggest that individuals have a right to information beyond their personal information. Further, the very definition of "aggregate consumer information" requires that the data not be reasonably linkable to any household.

Alternatively, if the intent of section 999.318(a) is to permit an individual consumer to obtain the collective categories of personal information about all consumers living in a particular household, NMHC believes this violates the privacy rights of other members in the household. This concern is particularly relevant to the multifamily industry where businesses regularly collect information on individuals living together in a household who are not necessarily

individuals of the same family or otherwise related. For example, it is common in our industry for students, military members, and other individuals to occupy a single dwelling. In fact, almost one-fifth (18 percent) of apartment households are comprised of non-family households, such as roommates.[6] Further, even members of the same family could be at risk if only one individual is needed to make a request (*e.g.*, an estranged spouse still living in the household). Permitting an individual to obtain information on all members of the household, even information in the aggregate or general categories of personal information, would violate the privacy rights of other individuals living in the household.

As written, NMHC believes the Proposed Regulations could enable an individual to obtain sensitive information (*e.g.*, a resident's legal status) on another individual living in the household without that individual's knowledge or consent. To illustrate, consider the following scenario. Two college students occupy a household in a privately owned and managed student housing community. One student initiates a request to know as it pertains to household information. In response, the business confirms that it collects various categories of information on the household, including criminal history, which can include complaints filed against members of the household. The consumer who initiated the request has never been involved with a criminal proceeding or been made aware of any complaints filed against her. Therefore, she may be able to infer that a criminal complaint was filed related to her roommate, even without accessing the specific information related to such reports.

B. Joint Household Requests

The following sets forth NMHC's comments related to joint household requests to know and requests to delete.

1. Proposed Regulations: § 999.318(b)

The same concerns set forth above also arise with respect to section 999.318(b), which would require a business to provide specific pieces of information, or delete household personal information, in response to a joint request by a household. Although the section states the requirement is subject to the Article 4 verification requirements, NMHC believes further clarity is needed in order to protect the privacy of all individuals residing in a household.

2. NMHC Request and Recommendation

NMHC recommends that section 999.318(b) be amended to make clear that (1) each adult member of the household must authorize the access or deletion request; (2) the business must verify the identities of each adult member making the request; and (3) the business must verify that each member of the household covered by the request is currently a member of the household. Proposed language is as follows:

[6] NMHC tabulations of 2018 American Community Survey microdata

999.318

~~*(a) Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.*~~

(b) If all consumers of the household jointly request access to ~~specific pieces~~ categories of personal information for the household or the deletion of household personal information, ~~and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4,~~ then the business shall comply with the request only if (a) the business can verify that each adult member of the household authorized the request; (b) the business can individually verify the identities of each adult member of the household making the request, subject to verification requirements set forth in Article 4; and (c) the business can verify that each member of the household to whom the request pertains is currently a member of the household.

CONCLUSION

The security and privacy of consumer information is a top priority to the multifamily industry. While the Proposed Regulations are certainly well-intentioned, NMHC believes the language as currently written inadvertently creates new risks to the privacy and security of consumer data. NMHC believes these concerns can be addressed through further amendment to the Proposed Regulations, as set forth above.

NMHC appreciates the opportunity to present the views of the multifamily industry in connection with the continued development and implementation of the CCPA. NMHC shares the same goal of protecting consumers' privacy and stands ready to work with the Attorney General to ensure the CCPA serves as an effective standard that recognizes the unique nature and needs of the rental housing industry while ensuring consumers' privacy rights are protected.

Sincerely,

Doug Bibby
President
National Multifamily Housing Council