DATA SECURITY

NMHC/NAA Viewpoint

As Congress continues to pursue data breach and cybersecurity legislation, NMHC/NAA encourages the adoption of reasonable approaches to safeguard consumer privacy and thwart cyberattacks.

Multifamily firms collect, use and maintain vast amounts of highly sensitive, personal data about residents, prospective residents and employees. Whether in paper or digital formats, the data collected is valuable to data thieves and those wishing to do harm to a company's reputation and financial standing. Personal information typically includes residents' names, addresses, Social Security numbers and driver's license numbers as well as additional information found in rental applications, leases, financial statements and insurance records.

The apartment industry has shifted from storing records as hard paper copies to web-based, digital documents, and the technology they are utilizing to do so is changing. Third-party payment processing systems enable residents to pay their rent online, creating efficiencies while adding convenience for residents. However, they are also a potential additional point of exposure for information theft unless protective measures are in place.

The increased reliance on technology and its always-advancing nature has led many to think of data breaches strictly in terms of external cyberattacks. Yet human error and negligence remain the largest cause of breached data. The portability of a tablet, laptop or smartphone, increases the chances of a device—and thus its con-tents—being lost or stolen.

To date, 47 states and the District of Columbia have state data breach laws mandating certain security and disclosure requirements.

Congress has placed the issues of cybersecurity and consumer privacy high on its agenda. Despite bipartisan agreement that data breach legislation is needed, there is a lack of consensus over the specifics of such a bill, including the scope of personally identifiable information, the definition of a breach and the timeframe for notifying the consumer about a breach. Some bills would create a national standard for data privacy protection and the breach notification process. Cybersecurity proposals are much broader and focus on protecting the nation's critical infrastructure but may be used to advance data breach measures.

NMHC/NAA support reasonable efforts to safeguard a consumer's personal information. Efforts should be limited to those situations in which there exists a real threat of identity theft so as to not unnecessarily overburden companies with notification obligations in situations that may not warrant such action.

NMHC/NAA Joint Legislative Program
1850 M Street, NW, Suite 540 | Washington, DC 20036 | 202 974 2300 WeAreApartments.org