STATE OF NEW YORK

48

2023-2024 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 4, 2023

Introduced by M. of A. L. ROSENTHAL, DINOWITZ, GLICK, SIMON, EPSTEIN, McMAHON, COLTON, WEPRIN -- read once and referred to the Committee on Housing

AN ACT to amend the multiple dwelling law and the multiple residence law, in relation to the use of electronic or computerized entry systems and the information that may be gathered from such systems

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The multiple dwelling law is amended by adding a new section 50-b to read as follows:

§ 50-b. Electronic or computerized entry systems. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(a) "Account information" means information that is used to grant a user entry or access to any online tools that are used to manage user accounts related to an electronic and/or computerized entry system.

(b) "Authentication data" means data generated or collected at a point of authentication in connection with granting a user entry to a class A multiple dwelling or common area with an electronic or computerized entry system, except that "authentication data" shall not include data generated through or collected by a video or camera system that is used to monitor entrances but not to grant entry.

(c) "Critical security vulnerability" means a security vulnerability that has a significant risk of resulting in an unauthorized access to an area secured by an electronic and/or computerized entry system.

(d) "Reference data" means information against which authentication data is verified at a point of authentication by a smart access system in order to grant a user entry to a smart access building or common area of such building.

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD00692-01-3

(e) "Security breach" means any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing underlying security mechanisms. A "security breach" occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical information technology perimeter.

2. Entry. a. Where a landlord installs or plans to install an electronic or computerized entry system on any entrance from the street, passageway, court, yard, cellar, or other common area of a class A multiple dwelling, such system shall not rely solely on a web-based application to facilitate entrance but shall also include a key fob, key card, digital key or passcode for tenant use.

b. Landlords may provide various methods of entry into individual apartments including a mechanical key or an electronic or computerized entry system of a key fob, key card or digital key, provided, however that such electronic or computerized entry system shall not rely solely on a web-based application.

c. Notwithstanding paragraph a or b of this subdivision, landlords shall provide a non-electronic means of entry where requested by the tenant due to a religious preference.

d. All lawful tenants and occupants shall be provided with a key, key fob, digital key or key card at no cost to such tenants. The term "occupants" shall include children under the age of eighteen who shall be issued a key, key fob, digital key or key card if a parent or guardian requests such child be provided with one. Tenants may also receive up to four additional keys, key fobs, digital key or key cards at no cost to the tenant for employees or guests. The term "guests" shall include family members and friends who can reasonably be expected to visit on a regular basis or visit as needed to care for the tenant or the apartment if the tenant is away. Employees, including contractors, professional caregivers or other services providers, may have an expiration date placed on their key, key card, digital key or key fob, which may be extended upon the tenant's or occupant's request. Tenants may request a new or replacement key, key fob, digital key or key card at any time throughout the course of the tenancy. The landlord or his or her agent shall provide the first replacement key, key fob, digital key or key card to the tenant free of charge. The cost of second and subsequent replacement cards shall not be more than what the landlord paid for the replacement up to and not exceeding twenty-five dollars.

e. The landlord shall not set limits on the number of keys, key fobs, digital keys or key cards a lawful tenant or occupant may request.

f. Any door that has an electronic or computerized entry system shall have backup power or an alternative means of entry to ensure that the entry system continues to operate during a power outage. A landlord, or his or her agent, shall routinely inspect the backup power and shall replace according to system specifications. Owners or their agents shall provide lawful tenants and occupants with information about whom to contact in the event that the tenant, occupant or the tenant's or occupant's children, guests or employees become locked out.

3. Notice. Landlords or their agents shall provide notice to a tenant at the time the tenant signs the lease, or when the electronic or computerized entry system is installed, of the provisions of subdivision two of this section.

4. Data collection. a. If an electronic and/or computerized entry system is utilized to gain entrance to a class A multiple dwelling, the only reference, authentication, and account information gathered by any electronic and/or computerized entry system shall be limited to account

information used to grant a user entry or to access any online tools used to manage user accounts related to the electronic and/or computerized entry system, or reference data, such as the lessee or tenant's name, apartment number, the preferred method of contact for such lessee or tenant, other doors or common areas to which the user has access, move-in and, if available move-out dates, and authentication data such as time and method of access for security purposes and a photograph of access events for security purposes. For electronic and computerized entry systems that rely on the collection of biometric data and which have already been installed at the time this section shall have become a law, a biometric identifier may be collected pursuant to this section in order to register a lessee or tenant for an electronic and/or computerized entry system. No new electronic and/or computerized entry systems that rely on the collection of biometric data shall be installed in class A multiple dwellings for three years after the effective date of this section.

(i) The owner of the multiple dwelling may collect only the minimum data required by the technology used in the electronic and/or computerized entry system to effectuate such entrance and protect the privacy and security of such tenants.

(ii) The owner or agent of the owner shall not request or retain, in any form, the social security number of any tenant or occupant as a condition of use of the electronic or computerized entry system.

(iii) The owner, agent of the owner, or the vendor of an electronic or computerized entry system on behalf of the owner may record each time a key fob, key card, digital key or passcode is used to enter the building, but shall not record any departures.

(iv) A copy of such data may be retained for reference at the point of authentication by the electronic and/or computerized entry system. Such reference data may be retained only for tenants or those authorized by the tenant or owner of the multiple dwelling.

(v) The owner of the multiple dwelling shall destroy or anonymize authentication data within a reasonable time, but not later than ninety days after the date collected.

(vi) Reference data for a tenant or those authorized by a tenant shall be destroyed or anonymized within ninety days of (1) the tenant permanently vacating the dwelling, or (2) a request by the tenant to withdraw authorization for those previously authorized by the tenant.

b. (i) For the purposes of this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand, face geometry or other similar feature.

(ii) An entity may not capture a biometric identifier of an individual to gain entrance to a class A multiple dwelling unless the person is a tenant or person authorized by the tenant, and informs the individual before capturing the biometric identifier; and receives their express consent to capture the biometric identifier.

(iii) Any entity that possesses a biometric identifier of an individual that is captured to gain entrance to a class A multiple dwelling:

(1) May not sell, lease or otherwise disclose the biometric identifier to another person unless pursuant to a grand jury subpoena or court ordered warrant, subpoena, or other authorized court ordered process.

(2) Shall store, transmit and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits and protects confidential information the person possesses; and

(3) Shall destroy the biometric identifier within a reasonable time, but not later than forty-eight hours after the date collected, except for reference data. If any prohibited information is collected, such as the likeness of a minor or a non-tenant, the information shall be destroyed immediately.

c. The owner of the multiple dwelling, or the managing agent, must develop written procedures which describe the process used to add persons authorized by the tenant to electronic and/or computerized entry systems on a temporary or permanent basis, such as visitors, children, their employees, and caregivers to such building.

(i) The procedures must clearly establish the owner's retention schedule and guidelines for permanently destroying or anonymizing the data collected.

(ii) The procedures cannot limit time or place of entrance by such people authorized by the tenant except as requested by the tenant.

5. Prohibitions. a. No form of location tracking, including but not limited to satellite location based services, shall be included in any equipment, key, or software provided to tenants or guests as part of an electronic and/or computerized entry system.

b. It shall be prohibited to collect through an electronic and/or computerized entry system the likeness of a minor occupant, information on the relationship status of tenants, lessees and/or guests, or to use a smart access system to collect or track information about the frequency and time of use of such system by a tenant and/or guests to harass or evict a tenant or for any other purpose not expressly related to the operation of the smart access system.

c. Information that is acquired via the use of an electronic and/or computerized entry system shall not be used for any purposes other than monitoring building entrances and shall not be used as the basis or support for an action to evict a lessee or tenant, or an administrative hearing seeking a change in regulatory coverage for an individual or unit. However, a tenant may authorize their information to be used by a third party, but such a request must clearly state who will have access to such information, for what purpose it will be used, and the privacy policies which will protect their information. Under no circumstances may a lease or a renewal be contingent upon authorizing such use. Electronic and/or computerized systems may use third-party services to the extent required to maintain and operate system infrastructure, including cloud-based hosting and storage. The provider or providers of third-party infrastructure services must meet or exceed the privacy protections set forth in this section and will be subject to the same liability for breach of any of the requirements of this section.

d. Information and data collected shall not be made available to any third party, unless authorized as described above, including but not limited to law enforcement, except upon a grand jury subpoena or a court ordered warrant, subpoena, or other authorized court ordered process.

6. Storage of information. Any information or data collected shall be stored in a secure manner to prevent unauthorized access by both employees and contractors and those unaffiliated with the landlord or their agents, except as otherwise provided in this section. Future or continuing tenancy shall not be conditioned upon consenting to the use of an electronic and/or computerized entry system.

7. Software issues. Whenever a company that produces, makes available or installs electronic or computerized entry systems discovers a security breach or critical security vulnerability in their software, such company shall notify customers of such vulnerability within a reasonable

time of discovery but no later than twenty-four hours after discovery and shall make software updates available and take any other action as may be necessary to repair the vulnerability within a reasonable time, but not longer than thirty days after discovery. Smart access systems and vendors shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected. In the event that a security breach or critical security vulnerability that pertains to the embedded software or firmware on the smart access systems is discovered, smart access systems and their vendors shall:

a. be able to create updates to the firmware to correct the vulnerabilities;

b. contractually commit to customers that the smart access system or vendor will create updates to the embedded software or firmware to remedy the vulnerabilities; and

c. make such security-related software or firmware updates available for free to customers for the duration of the contract between smart access buildings and smart access systems.

8. Waiver of rights; void. Any agreement by a lessee or tenant of a dwelling waiving or modifying his or her rights as set forth in this section shall be void as contrary to public policy.

9. Penalties. (a) A person who violates this section is subject to a civil penalty of not more than five thousand dollars for each violation. The attorney general may bring an action to recover the civil penalty. An individual injured by a violation of this section may bring an action to recover damages. A court may also award attorneys' fees to a prevailing plaintiff.

(b) Where a landlord or his or her agent uses an electronic or computerized entry system to harass or otherwise deprive a tenant of any rights available under law, such landlord or agent shall be subject to a civil penalty of ten thousand dollars for each violation.

(c) For purposes of this subdivision, each day the violation occurs shall be considered a separate violation.

10. Rent regulated dwellings. Installation of an electronic or computerized entry system pursuant to this section in a rent regulated dwelling shall constitute a modification of services requiring the landlord of such dwelling or his or her agent to apply to the division of housing and community renewal for approval before performing such installation. Such installation shall not qualify as a basis for rent reduction.

11. Exemptions. a. Nothing herein shall apply to multiple dwellings owned or managed by an entity subject to 42 U.S.C. § 1437 et seq., or any of its subsidiaries.

b. Nothing in this section shall limit the authority of the division of housing and community renewal to impose additional requirements regarding electronic or computerized entry systems installed in multiple dwellings for which the division is required to approve substitutions or modifications of services.

§ 2. The multiple residence law is amended by adding a new section 130-a to read as follows:

§ 130-a. Electronic or computerized entry systems. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(a) "Account information" means information that is used to grant a user entry or access to any online tools that are used to manage user accounts related to an electronic and/or computerized entry system.

(b) "Authentication data" means data generated or collected at a point of authentication in connection with granting a user entry to a class A

multiple dwelling or common area with an electronic or computerized entry system, except that "authentication data" shall not include data generated through or collected by a video or camera system that is used to monitor entrances but not to grant entry.

(c) "Critical security vulnerability" means a security vulnerability that has a significant risk of resulting in an unauthorized access to an area secured by an electronic and/or computerized entry system.

(d) "Reference data" means information against which authentication data is verified at a point of authentication by a smart access system in order to grant a user entry to a smart access building or common area of such building.

(e) "Security breach" means any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing underlying security mechanisms. A "security breach" occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical information technology perimeter.

2. Entry. (a) Where a landlord installs or plans to install an electronic or computerized entry system on any entrance from the street, passageway, court, yard, cellar, or other common area of a class A multiple dwelling, such system shall not rely solely on a web-based application to facilitate entrance but shall also include a key fob, key card, digital key or passcode for tenant use.

(b) Landlords may provide various methods of entry into individual apartments including a mechanical key or an electronic or computerized entry system of a key fob, key card or digital key, provided, however that such electronic or computerized entry system shall not rely solely on a web-based application.

(c) Notwithstanding paragraph (a) or (b) of this subdivision, landlords shall provide a non-electronic means of entry where requested by the tenant due to a religious preference.

(d) All lawful tenants and occupants shall be provided with a key, key fob, digital key or key card at no cost to such tenants. The term "occupants" shall include children under the age of eighteen who shall be issued a key, key fob, digital key or key card if a parent or guardian requests such child be provided with one. Tenants may also receive up to four additional keys, key fobs, digital key or key cards at no cost to the tenant for employees or guests. The term "guests" shall include family members and friends who can reasonably be expected to visit on a regular basis or visit as needed to care for the tenant or the apartment if the tenant is away. Employees, including contractors, professional caregivers or other services providers, may have an expiration date placed on their key, key card, digital key or key fob, which may be extended upon the tenant's or occupant's request. Tenants may request a new or replacement key, key fob, digital key or key card at any time throughout the course of the tenancy. The landlord or his or her agent shall provide the first replacement key, key fob, digital key or key card to the tenant free of charge. The cost of second and subsequent replacement cards shall not be more than what the landlord paid for the replacement up to and not exceeding twenty-five dollars.

(e) The landlord shall not set limits on the number of keys, key fobs, digital keys or key cards a lawful tenant or occupant may request.

(f) Any door that has an electronic or computerized entry system shall have backup power or an alternative means of entry to ensure that the entry system continues to operate during a power outage. A landlord, or his or her agent, shall routinely inspect the backup power and shall replace according to system specifications. Owners or their agents shall

provide lawful tenants and occupants with information about whom to contact in the event that the tenant, occupant or the tenant's or occupant's children, guests or employees become locked out.

3. Notice. Landlords or their agents shall provide notice to a tenant at the time the tenant signs the lease, or when the electronic or computerized entry system is installed, of the provisions of subdivision two of this section.

4. Data collection. (a) If an electronic and/or computerized entry system is utilized to gain entrance to a class A multiple dwelling, the only reference, authentication, and account information gathered by any electronic and/or computerized entry system shall be limited to account information used to grant a user entry or to access any online tools used to manage user accounts related to the electronic and/or computerized entry system, or reference data, such as the lessee or tenant's name, apartment number, the preferred method of contact for such lessee or tenant, other doors or common areas to which the user has access, move-in and, if available move-out dates, and authentication data such as time and method of access for security purposes and a photograph of access events for security purposes. For electronic and computerized entry systems that rely on the collection of biometric data and which have already been installed at the time this section shall have become a law, a biometric identifier may be collected pursuant to this section in order to register a lessee or tenant for an electronic and/or computerized entry system. No new electronic and/or computerized entry systems that rely on the collection of biometric data shall be installed in class A multiple dwellings for three years after the effective date of this section.

(i) The owner of the multiple dwelling may collect only the minimum data required by the technology used in the electronic and/or computerized entry system to effectuate such entrance and protect the privacy and security of such tenants.

(ii) The owner or agent of the owner shall not request or retain, in any form, the social security number of any tenant or occupant as a condition of use of the electronic or computerized entry system.

(iii) The owner, agent of the owner, or the vendor of an electronic or computerized entry system on behalf of the owner may record each time a key fob, key card, digital key or passcode is used to enter the building, but shall not record any departures.

(iv) A copy of such data may be retained for reference at the point of authentication by the electronic and/or computerized entry system. Such reference data may be retained only for tenants or those authorized by the tenant or owner of the multiple dwelling.

(v) The owner of the multiple dwelling shall destroy or anonymize authentication data within a reasonable time, but not later than ninety days after the date collected.

(vi) Reference data for a tenant or those authorized by a tenant shall be destroyed or anonymized within ninety days of (1) the tenant permanently vacating the dwelling, or (2) a request by the tenant to withdraw authorization for those previously authorized by the tenant.

(b) (i) For the purposes of this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand, face geometry or other similar feature.

(ii) An entity may not capture a biometric identifier of an individual to gain entrance to a class A multiple dwelling unless the person is a tenant or person authorized by the tenant, and informs the individual

before capturing the biometric identifier; and receives their express consent to capture the biometric identifier.

(iii) Any entity that possesses a biometric identifier of an individual that is captured to gain entrance to a class A multiple dwelling:

(1) May not sell, lease or otherwise disclose the biometric identifier to another person unless pursuant to a grand jury subpoena or court ordered warrant, subpoena, or other authorized court ordered process.

(2) Shall store, transmit and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits and protects confidential information the person possesses; and

(3) Shall destroy the biometric identifier within a reasonable time, but not later than forty-eight hours after the date collected, except for reference data. If any prohibited information is collected, such as the likeness of a minor or a non-tenant, the information shall be destroyed immediately.

(c) The owner of the multiple dwelling, or the managing agent, must develop written procedures which describe the process used to add persons authorized by the tenant to electronic and/or computerized entry systems on a temporary or permanent basis, such as visitors, children, their employees, and caregivers to such building.

(i) The procedures must clearly establish the owner's retention schedule and guidelines for permanently destroying or anonymizing the data collected.

(ii) The procedures cannot limit time or place of entrance by such people authorized by the tenant except as requested by the tenant.

5. Prohibitions. (a) No form of location tracking, including but not limited to satellite location based services, shall be included in any equipment, key, or software provided to tenants or guests as part of an electronic and/or computerized entry system.

(b) It shall be prohibited to collect through an electronic and/or computerized entry system the likeness of a minor occupant, information on the relationship status of tenants, lessees and/or guests, or to use a smart access system to collect or track information about the frequency and time of use of such system by a tenant and/or guests to harass or evict a tenant or for any other purpose not expressly related to the operation of the smart access system.

(c) Information that is acquired via the use of an electronic and/or computerized entry system shall not be used for any purposes other than monitoring building entrances and shall not be used as the basis or support for an action to evict a lessee or tenant, or an administrative hearing seeking a change in regulatory coverage for an individual or unit. However, a tenant may authorize their information to be used by a third party, but such a request must clearly state who will have access to such information, for what purpose it will be used, and the privacy policies which will protect their information. Under no circumstances may a lease or a renewal be contingent upon authorizing such use. Electronic and/or computerized systems may use third-party services to the extent required to maintain and operate system infrastructure, including cloud-based hosting and storage. The provider or providers of third-party infrastructure services must meet or exceed the privacy protections set forth in this section and will be subject to the same liability for breach of any of the requirements of this section.

(d) Information and data collected shall not be made available to any third party, unless authorized as described above, including but not

limited to law enforcement, except upon a grand jury subpoena or a court ordered warrant, subpoena, or other authorized court ordered process.

6. Storage of information. Any information or data collected shall be stored in a secure manner to prevent unauthorized access by both employees and contractors and those unaffiliated with the landlord or their agents, except as otherwise provided in this section. Future or continuing tenancy shall not be conditioned upon consenting to the use of an electronic and/or computerized entry system.

7. Software issues. Whenever a company that produces, makes available or installs electronic or computerized entry systems discovers a security breach or critical security vulnerability in their software, such company shall notify customers of such vulnerability within a reasonable time of discovery but no later than twenty-four hours after discovery and shall make software updates available and take any other action as may be necessary to repair the vulnerability within a reasonable time, but not longer than thirty days after discovery. Smart access systems and vendors shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected. In the event that a security breach or critical security vulnerability that pertains to the embedded software or firmware on the smart access systems is discovered, smart access systems and their vendors shall:

(a) be able to create updates to the firmware to correct the vulnerabilities;

(b) contractually commit to customers that the smart access system or vendor will create updates to the embedded software or firmware to remedy the vulnerabilities; and

(c) make such security-related software or firmware updates available for free to customers for the duration of the contract between smart access buildings and smart access systems.

8. Waiver of rights; void. Any agreement by a lessee or tenant of a dwelling waiving or modifying his or her rights as set forth in this section shall be void as contrary to public policy.

9. Penalties. (a) A person who violates this section is subject to a civil penalty of not more than five thousand dollars for each violation. The attorney general may bring an action to recover the civil penalty. An individual injured by a violation of this section may bring an action to recover damages. A court may also award attorneys' fees to a prevailing plaintiff.

(b) Where a landlord or his or her agent uses an electronic or computerized entry system to harass or otherwise deprive a tenant of any rights available under law, such landlord or agent shall be subject to a civil penalty of ten thousand dollars for each violation.

(c) For purposes of this subdivision, each day the violation occurs shall be considered a separate violation.

10. Rent regulated dwellings. Installation of an electronic or computerized entry system pursuant to this section in a rent regulated dwelling shall constitute a modification of services requiring the landlord of such dwelling or his or her agent to apply to the division of housing and community renewal for approval before performing such installation. Such installation shall not qualify as a basis for rent reduction.

11. Exemptions. (a) Nothing herein shall apply to multiple dwellings owned or managed by an entity subject to 42 U.S.C. § 1437 et seq., or any of its subsidiaries.

(b) Nothing in this section shall limit the authority of the division of housing and community renewal to impose additional requirements regarding electronic or computerized entry systems installed in multiple

dwellings for which the division is required to approve substitutions or modifications of services.

§ 3. Severability. If any provision of this act, or any application of any provision of this act, is held to be invalid, that shall not affect the validity or effectiveness of any other provision of this act, or of any other application of any provision of this act, which can be given effect without that provision or application; and to that end, the provisions and applications of this act are severable.

§ 4. This act shall take effect on the one hundred eightieth day after it shall have become a law.