

# STATE OF NEW YORK

6463--A

2021-2022 Regular Sessions

## IN SENATE

April 29, 2021

Introduced by Sens. KAVANAGH, KRUEGER -- read twice and ordered printed, and when printed to be committed to the Committee on Housing, Construction and Community Development -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

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:

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

3 § 50-b. Electronic or computerized entry systems. 1. Definitions. For  
4 the purposes of this section, the following terms shall have the follow-  
5 ing meanings:

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

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

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

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

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

LBD00549-07-1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

47 (iii) Any entity that possesses a biometric identifier of an individ-  
48 ual that is captured to gain entrance to a class A multiple dwelling:

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

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

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

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

11     (i) The procedures must clearly establish the owner's retention sched-  
12 ule and guidelines for permanently destroying or anonymizing the data  
13 collected.

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

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

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

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

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

47     6. Storage of information. Any information or data collected shall be  
48 stored in a secure manner to prevent unauthorized access by both employ-  
49 ees and contractors and those unaffiliated with the landlord or their  
50 agents, except as otherwise provided in this section. Future or continu-  
51 ing tenancy shall not be conditioned upon consenting to the use of an  
52 electronic and/or computerized entry system.

53     7. Software issues. Whenever a company that produces, makes available  
54 or installs electronic or computerized entry systems discovers a securi-  
55 ty breach or critical security vulnerability in their software, such  
56 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 (iii) Any entity that possesses a biometric identifier of an individ-  
4 ual that is captured to gain entrance to a class A multiple dwelling:

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

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

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

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

22 (i) The procedures must clearly establish the owner's retention sched-  
23 ule and guidelines for permanently destroying or anonymizing the data  
24 collected.

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

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

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

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

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

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

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

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

22 (a) be able to create updates to the firmware to correct the vulner-  
23 abilities;

24 (b) contractually commit to customers that the smart access system or  
25 vendor will create updates to the embedded software or firmware to reme-  
26 dy the vulnerabilities; and

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

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

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

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

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

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

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

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

1 dwelling for which the division is required to approve substitutions or  
2 modifications of services.

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

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