

STATE OF NEW YORK

706--C

2021-2022 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 6, 2021

Introduced by M. of A. L. ROSENTHAL, DINOWITZ, EPSTEIN, SIMON, GLICK, GALEF, J. RIVERA, McMAHON, GOTTFRIED, FRONTUS, ABINANTI, COLTON, WEPRIN -- read once and referred to the Committee on Housing -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- again reported from said committee with amendments, ordered reprinted as amended and recommitted to said committee -- again reported from said committee with amendments, 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.

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

LBD00549-06-1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 a. be able to create updates to the firmware to correct the vulner-
15 abilities;

16 b. contractually commit to customers that the smart access system or
17 vendor will create updates to the embedded software or firmware to reme-
18 dy the vulnerabilities; and

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

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

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

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

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

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

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

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

51 § 2. The multiple residence law is amended by adding a new section
52 130-a to read as follows:

53 § 130-a. Electronic or computerized entry systems. 1. Definitions. For
54 the purposes of this section, the following terms shall have the follow-
55 ing meanings:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 ty infrastructure services must meet or exceed the privacy protections
2 set forth in this section and will be subject to the same liability for
3 breach of any of the requirements of this section.

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

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

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

27 (a) be able to create updates to the firmware to correct the vulner-
28 abilities;

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

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

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

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

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

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

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

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

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

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

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