

STATE OF NEW YORK

4374

2023-2024 Regular Sessions

IN ASSEMBLY

February 14, 2023

Introduced by M. of A. GUNTHER, SAYEGH, THIELE, DICKENS, DARLING, ZEBROWSKI, CRUZ, HYNDMAN, GLICK, JONES, DeSTEFANO, SMULLEN, J. M. GIGLIO, McDONOUGH, PAULIN -- read once and referred to the Committee on Consumer Affairs and Protection

AN ACT to amend the general business law and the state finance law, in relation to allowing consumers the right to request from businesses the categories of personal information the business has sold or disclosed to third parties

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

1 Section 1. The article heading of article 39-F of the general business
2 law, as amended by chapter 117 of the laws of 2019, is amended to read
3 as follows:

4 [~~NOTIFICATION OF UNAUTHORIZED~~] ACQUISITION AND CONTROL
5 OF PRIVATE AND PERSONAL INFORMATION; DATA SECURITY
6 PROTECTIONS

7 § 2. The general business law is amended by adding a new section 899-
8 cc to read as follows:

9 § 899-cc. Consumer control of personal information. 1. For purposes of
10 this section, the following definitions shall apply:

11 (a) "Biometric data" means an individual's physiological, biological
12 or behavioral characteristics, including an individual's deoxyribonu-
13 cleic acid that can be used, singly or in combination with each other or
14 with other identifying data to establish individual identity. Biometric
15 data includes but is not limited to imagery of the iris, retina, finger-
16 print, face, hand, palm, vein patterns, and voice recordings, from which
17 an identifier template, such as a faceprint, a minutiae template, or a
18 voiceprint, can be extracted, and keystroke patterns or rhythms, gait

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

LBD07607-01-3

1 patterns or rhythms, and sleep, health, or exercise data that contain
2 identifying information.

3 (b) "Business" means:

4 (1) a sole-proprietorship, partnership, limited-liability company,
5 corporation, association, or other legal entity that is organized or
6 operated for the profit or financial benefit of its shareholders or
7 other owners, that collects consumers' personal information, that does
8 business in the state, and that satisfies one or more of the following
9 thresholds: (A) has annual gross revenues in excess of fifty million
10 dollars, as adjusted pursuant to subparagraph five of paragraph (a) of
11 subdivision fifteen of this section; or (B) annually sells, alone or in
12 combination, the personal information of one hundred thousand or more
13 consumers or devices; or (C) derives fifty percent or more of its annual
14 revenues from selling consumers' personal information; and

15 (2) any entity that controls or is controlled by a business, as
16 defined in paragraph one of this subdivision, and that shares common
17 branding with the business. "Control" or "controlled" means ownership
18 of, or the power to vote, more than fifty percent of the outstanding
19 shares of any class of voting security of a business; control in any
20 manner over the election of a majority of the directors, or of individ-
21 uals exercising similar functions; or the power to exercise, directly or
22 indirectly, a controlling influence over the management or policies of a
23 company. "Common branding" means a shared name, servicemark, or trade-
24 mark.

25 (c) "Business purpose" means the use of personal information for the
26 business's operational purposes, provided that the use of personal
27 information shall be reasonably necessary and proportionate to achieve
28 the operational purpose for which it is specifically permitted. Unrea-
29 sonable or disproportionate use shall not be considered a "business
30 purpose". Business purposes are:

31 (1) Auditing related to a current interaction with the consumer and
32 concurrent transactions, including but not limited to, counting ad
33 impressions to unique visitors, verifying positioning and quality of ad
34 impressions and auditing compliance with this specification and other
35 standards;

36 (2) Detecting security incidents, protecting against malicious, decep-
37 tive, fraudulent, or illegal activity, and prosecuting those responsible
38 for such activity;

39 (3) Debugging to identify and repair errors that impair existing
40 intended functionality;

41 (4) Short-term, transient use, provided the personal information is
42 not disclosed to another person and is not used to build a profile about
43 a consumer or otherwise alter an individual consumer's experience
44 outside the current interaction, including but not limited to, the
45 contextual customization of ads shown as part of the same interaction;
46 and

47 (5) Performing services on behalf of the business, including maintain-
48 ing or servicing accounts, providing customer service, processing or
49 fulfilling orders and transactions, verifying customer information,
50 processing payments, providing financing, providing advertising or
51 marketing services, providing analytical services, or providing similar
52 services on behalf of the business.

53 (d) "Clear and conspicuous" means (1) in a color that contrasts with
54 the background color or is otherwise distinguishable; (2) written in
55 larger type than the surrounding text and in a fashion that calls atten-

tion to the language; and (3) prominently displayed so that a reasonable viewer would be able to notice, read, and understand it.

(e) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" does not include for the purpose of engaging in speech that state or federal courts have recognized as non-commercial speech, including political speech and journalism.

(f) "Collects", "collected" or "collection" means buying, renting, gathering, obtaining, storing, using, monitoring, accessing, or making inferences based upon, any personal information pertaining to a consumer by any means.

(g) "Consumer" means a natural person who is a resident of the state.

(h) "De-identified" means information that cannot reasonably identify, relate to, describe, reference, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer or device, provided that a business that uses de-identified information: (1) has implemented technical safeguards that prohibit re-identification of the consumer or consumers to whom the information may pertain; (2) has implemented business processes that specifically prohibit re-identification of the information; (3) has implemented business processes to prevent inadvertent release of de-identified information; and (4) makes no attempt to re-identify the information.

(i) "Designated methods for submitting requests" means a mailing address, e-mail address, web page, web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this section. If the consumer does not maintain an account with the business, the business shall provide an opportunity for the consumer to designate whether the consumer wishes to receive the information required to be disclosed pursuant to subdivisions two and three of this section by mail or electronically, at the consumer's option.

(j) "Homepage" means the introductory page of a website and any webpage where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page, a link within the application, such as from the application configuration, "about", "information", or settings page, and any other location that allows consumers to review the notice required by paragraph (a) of subdivision seven of this section, including but not limited to, before downloading the application.

(k) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(l) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(m) (1) "Personal information" means information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device, including, but not limited to:

(A) any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, alias, signature, social security

number, physical characteristics or description, address, electronic mail address, internet protocol address, unique identifier, account name, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information;

(B) characteristics of protected classifications under state or federal law;

(C) commercial information, including records of property, products or services provided, obtained, or considered, or other purchasing or consuming histories or tendencies;

(D) biometric data;

(E) internet or other electronic network activity information, including but not limited to, browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;

(F) geolocation data;

(G) audio, electronic, visual, thermal, olfactory, or similar information;

(H) psychometric information;

(I) professional or employment-related information;

(J) inferences drawn from any of the information identified above; and

(K) any of the categories of information set forth in this subdivision as they pertain to the minor children of the consumer.

(2) "Personal information" does not include information that is publicly available or that is de-identified.

(n) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in subparagraph one of paragraph (m) of this subdivision.

(o) "Psychometric information" means information derived or created from the use or application of psychometric theory or psychometrics, whereby through the use of any method, model, tool, or formula, observable phenomena, such as actions or events, are connected, measured, assessed, or related to a consumer's attributes, including, but not limited to, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(p) "Publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(q)(1) "Sell", "selling", "sale" or "sold" means: (A) selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for valuable consideration; or (B) sharing orally, in writing, or by electronic or other means, a consumer's personal information with a third party, whether for valuable consideration or for no consideration, for the third party's commercial purposes.

(2) For purposes of this section, a business does not sell personal information when:

(A) A consumer uses the business: (i) to intentionally disclose personal information, or (ii) to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to

1 interact with the third party via one or more deliberate interactions.
2 Hovering over, muting, pausing, or closing a given piece of content does
3 not constitute a consumer's intent to interact with a third party; or

4 (B) The business uses an identifier for a consumer who has opted out
5 of the sale of the consumer's personal information for the purposes of
6 alerting third parties that the consumer has opted out of the sale of
7 the consumer's personal information.

8 (r) "Service" or "services" means work, labor, and services, including
9 services furnished in connection with the sale or repair of goods.

10 (s) "Third party" means any person who is not:

11 (1) The business that collects personal information from consumers
12 under this section; or

13 (2) A person to whom the business discloses a consumer's personal
14 information for a business purpose pursuant to a written contract,
15 provided that the contract:

16 (A) Prohibits the person receiving the personal information from: (i)
17 selling the personal information; (ii) retaining, using, or disclosing
18 the personal information for any purpose other than for the specific
19 purpose of performing the services specified in the contract, including
20 retaining, using, or disclosing the personal information for a commer-
21 cial purpose other than providing the services specified in the
22 contract; and (iii) retaining, using, or disclosing the information
23 outside of the direct business relationship between the person and the
24 business; and

25 (B) Includes a certification made by the person receiving the personal
26 information that the person understands the restrictions in clause (A)
27 of this subparagraph and will comply with them. A person covered by this
28 subparagraph that violates any of the restrictions set forth in this
29 section shall be liable for such violations under this section. A busi-
30 ness that discloses personal information to a person covered by this
31 subparagraph in compliance with such subparagraph shall not be liable
32 under this section if the person receiving the personal information uses
33 it in violation of the restrictions set forth in this section, provided
34 that, at the time of disclosing the personal information, the business
35 does not have actual knowledge, or reason to believe, that the person
36 intends to commit such a violation.

37 (t) "Unique identifier" means a persistent identifier that can be used
38 to recognize a consumer or a device over time and across different
39 services, including but not limited to, a device identifier; internet
40 protocol address; cookies, beacons, pixel tags, mobile ad identifiers,
41 or similar technology; customer number, unique pseudonym, or user alias;
42 and telephone numbers, or other forms of persistent or probabilistic
43 identifiers that can be used to identify a particular consumer or
44 device.

45 (u) "Verifiable request" means a request that: (1) is made by a
46 consumer, by a consumer on behalf of the consumer's minor child, or by a
47 person authorized by the consumer to act on the consumer's behalf; and
48 (2) the business has verified, pursuant to regulations adopted by the
49 attorney general pursuant to subparagraph seven of paragraph (a) of
50 subdivision fifteen of this section, to be the consumer about whom the
51 business has collected personal information. A business is not obligated
52 to provide information to the consumer pursuant to subdivisions two and
53 three of this section if the business cannot verify, pursuant to this
54 subdivision and regulations adopted by the attorney general pursuant to
55 subparagraph seven of paragraph (a) of subdivision fifteen of this

1 section, that the consumer making the request is the consumer about whom
2 the business has collected information.

3 2. (a) A consumer shall have the right to request that a business that
4 collects personal information about the consumer disclose to the consum-
5 er the categories of personal information it has collected about that
6 consumer.

7 (b) A business that collects personal information about a consumer
8 shall disclose to the consumer, pursuant to subparagraph three of para-
9 graph (a) of subdivision six of this section, the information specified
10 in paragraph (a) of subdivision one of this section upon receipt of a
11 verifiable request from the consumer.

12 (c) A business that collects personal information about consumers
13 shall disclose, pursuant to clause (B) of subparagraph five of paragraph
14 (a) of subdivision six of this section, the categories of personal
15 information it has collected about consumers.

16 3. (a) A consumer shall have the right to request that a business that
17 sells the consumer's personal information, or that discloses it for a
18 business purpose, disclose to that consumer: (1) the categories of
19 personal information that the business sold about the consumer and the
20 identity of the third parties to whom such personal information was
21 sold, by category or categories of personal information for each third
22 party to whom such personal information was sold; and (2) the categories
23 of personal information that the business disclosed about the consumer
24 for a business purpose and the identity of the persons to whom such
25 personal information was disclosed for a business purpose, by category
26 or categories of personal information for each person to whom such
27 personal information was disclosed for a business purpose.

28 (b) A business that sells personal information about a consumer, or
29 that discloses a consumer's personal information for a business purpose,
30 shall disclose, pursuant to subparagraph four of paragraph (a) of subdi-
31 vision six of this section, the information specified in paragraph (a)
32 of this subdivision to the consumer upon receipt of a verifiable request
33 from the consumer.

34 (c) A business that sells consumers' personal information, or that
35 discloses consumers' personal information for a business purpose, shall
36 disclose, pursuant to clause (C) of subparagraph five of paragraph (a)
37 of subdivision six of this section: (1) the category or categories of
38 consumers' personal information it has sold; or if the business has not
39 sold consumers' personal information, it shall disclose that fact; and
40 (2) the category or categories of consumers' personal information it has
41 disclosed for a business purpose; or if the business has not disclosed
42 consumers' personal information for a business purpose, it shall
43 disclose that fact.

44 4. (a) A consumer shall have the right, at any time, to direct a busi-
45 ness that sells personal information about the consumer not to sell the
46 consumer's personal information. This right may be referred to as the
47 right to opt out.

48 (b) Notwithstanding paragraph (a) of this subdivision, a business
49 shall not sell the personal information of consumers if the business has
50 actual knowledge, or willfully disregards, that the consumer is less
51 than sixteen years of age, unless the consumer, in the case of consumers
52 thirteen, fourteen and fifteen years of age, or the consumer's parent or
53 guardian, in the case of consumers who are less than thirteen years of
54 age, has affirmatively authorized the sale of the consumer's personal
55 information. This right may be referred to as the right to opt in.

1 (c) A business that sells consumers' personal information shall
2 provide notice to consumers, pursuant to paragraph (a) of subdivision
3 seven of this section, that such information may be sold and that
4 consumers have the right to opt out of the sale of their personal infor-
5 mation.

6 (d) A business that has received direction from a consumer not to sell
7 the consumer's personal information, or, in the case of a minor consum-
8 er's personal information, has not received consent to sell the minor
9 consumer's personal information, shall be prohibited, pursuant to
10 subparagraph four of paragraph (a) of subdivision seven of this section,
11 from selling the consumer's personal information after its receipt of
12 the consumer's direction, unless the consumer subsequently provides
13 express authorization for the sale of the consumer's personal informa-
14 tion.

15 5. A business shall be prohibited from discriminating against a
16 consumer because the consumer requested information pursuant to subdivi-
17 sions two and three of this section, or because the consumer directed
18 the business not to sell the consumer's personal information pursuant to
19 subdivision four of this section, or because the consumer otherwise
20 exercised rights under this title, or exercised the consumer's rights to
21 enforce this section, including but not limited to, by: (a) denying
22 goods or services to the consumer; (b) charging different prices or
23 rates for goods or services, including through the use of discounts or
24 other benefits or imposing penalties; (c) providing a different level or
25 quality of goods or services to the consumer; or (d) suggesting that the
26 consumer will receive a different price or rate for goods or services,
27 or a different level or quality of goods or services, if the consumer
28 exercises the consumer's rights under this section.

29 6. (a) In order to comply with subdivisions two, three and five of
30 this section, a business shall:

31 (1) Make available to consumers two or more designated methods for
32 submitting requests for information required to be disclosed pursuant to
33 subdivisions two and three of this section, including, at a minimum, a
34 toll-free telephone number, and if the business maintains a website, a
35 website address.

36 (2) Disclose and deliver the required information to a consumer free
37 of charge within forty-five days of receiving a verifiable request from
38 the consumer. The business shall promptly take steps to determine wheth-
39 er the request is a verifiable request, but this shall not extend the
40 business's duty to disclose and deliver the information within forty-
41 five days of receipt of the consumer's request. The disclosure shall
42 cover the twelve-month period preceding the business's receipt of the
43 verifiable request and shall be made in writing and delivered through
44 the consumer's account with the business, if the consumer maintains an
45 account with the business, or by mail or electronically at the consum-
46 er's option if the consumer does not maintain an account with the busi-
47 ness. The business shall not require the consumer to create an account
48 with the business in order to make a verifiable request.

49 (3) For purposes of paragraph (b) of subdivision two of this section:
50 (A) identify the consumer, associate the information provided by the
51 consumer in the verifiable request to any personal information previous-
52 ly collected by the business about the consumer; and (B) identify by
53 category or categories the personal information collected about the
54 consumer in the preceding twelve months by reference to the enumerated
55 category or categories in paragraph (c) of this subdivision that most
56 closely describes the personal information collected.

(4) For purposes of paragraph (b) of subdivision three of this section: (A) identify the consumer, associate the information provided by the consumer in the verifiable request to any personal information previously collected by the business about the consumer; (B) identify by category or categories the personal information of the consumer that the business sold in the preceding twelve months by reference to the enumerated category or categories in paragraph (c) of this subdivision that most closely describes the personal information, and provide accurate names and contact information for the third parties to whom the consumer's personal information was sold in the preceding twelve months by reference to the enumerated category or categories in paragraph (c) of this subdivision that most closely describes the personal information sold for each third party; and (C) identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding twelve months by reference to the enumerated category or categories in paragraph (c) of this subdivision that most closely describes the personal information, and provide accurate names and contact information for the persons to whom the consumer's personal information was disclosed for a business purpose in the preceding twelve months by reference to the enumerated category or categories in paragraph (c) of this subdivision of this section that most closely describes the personal information disclosed for each person. The business shall disclose the information required by clauses (B) and (C) of this subparagraph in two separate lists.

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any New York-specific description of consumers' privacy rights, or if the business does not maintain such policies, on its website, and update such information at least once every twelve months:

(A) A description of a consumer's rights pursuant to subdivisions two, three and five of this section, and one or more designated methods for submitting requests;

(B) For purposes of paragraph (c) of subdivision two of this section, a list of the categories of personal information it has collected about consumers in the preceding twelve months by reference to the enumerated category or categories in paragraph (c) of this subdivision that most closely describes the personal information collected; and

(C) For purposes of subparagraphs one and two of paragraph (c) of subdivision three of this section, two separate lists: (i) a list of the categories of personal information it has sold about consumers in the preceding twelve months by reference to the enumerated category or categories in paragraph (c) of this subdivision that most closely describes the personal information sold, or if the business has not sold consumers' personal information in the preceding twelve months, the business shall disclose that fact; and (ii) a list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding twelve months by reference to the enumerated category or categories in paragraph (c) of this subdivision that most closely describes the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding twelve months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this section are informed of all requirements in this subdivision, as well as in subdivisions two, three and five of this

1 section, and how to direct consumers to exercise their rights under
2 those sections; and

3 (7) Use any personal information collected from the consumer in
4 connection with the business's verification of the consumer's request
5 solely for the purposes of verification.

6 (b) A business is not obligated to provide the information required by
7 subdivisions two and three of this section to the same consumer more
8 than once in a twelve-month period.

9 (c) The categories of personal information required to be disclosed
10 pursuant to subdivisions two and three of this section are all of the
11 following:

12 (1) Identifiers such as a real name, alias, postal address, unique
13 identifier, internet protocol address, electronic mail address, account
14 name, social security number, driver's license number, passport number,
15 or other similar identifiers;

16 (2) All categories of personal information enumerated in paragraph (a)
17 of subdivision one of this section;

18 (3) All categories of personal information relating to characteristics
19 of protected classifications under state or federal law, with specific
20 reference to the category of information that has been collected, such
21 as race, ethnicity, or gender;

22 (4) Commercial information, including records of property, products or
23 services provided, obtained, or considered, or other purchasing or
24 consuming histories or tendencies;

25 (5) Biometric data;

26 (6) Internet or other electronic network activity information, includ-
27 ing but not limited to, browsing history, search history, and informa-
28 tion regarding a consumer's interaction with a website, application, or
29 advertisement;

30 (7) Geolocation data;

31 (8) Audio, electronic, visual, thermal, olfactory, or similar informa-
32 tion;

33 (9) Psychometric information;

34 (10) Professional or employment-related information;

35 (11) Inferences drawn from any of the information identified above;
36 and

37 (12) Any of the categories of information set forth in this paragraph
38 as they pertain to the minor children of the consumer.

39 7. (a) A business that is required to comply with subdivision four of
40 this section shall:

41 (1) Provide a clear and conspicuous link on the business's homepage,
42 titled "Do Not Sell My Personal Information", to a webpage that enables
43 a consumer, or a person authorized by the consumer, to opt out of the
44 sale of the consumer's personal information. A business shall not
45 require a consumer to create an account in order to direct the business
46 not to sell the consumer's personal information;

47 (2) Include a description of a consumer's rights pursuant to subdivi-
48 sion four of this section, along with a separate link to the "Do Not
49 Sell My Personal Information" webpage in: (A) its online privacy policy
50 or policies if the business has an online privacy policy or policies,
51 and (B) any state specific description of consumers' privacy rights;

52 (3) Ensure that all individuals responsible for handling consumer
53 inquiries about the business's privacy practices or the business's
54 compliance with this section are informed of all requirements in this
55 subdivision as well as subdivision four of this section, and how to
56 direct consumers to exercise their rights under those sections;

1 (4) For consumers who exercise their right to opt out of the sale of
2 their personal information, refrain from selling personal information
3 collected by the business about the consumer;

4 (5) For a consumer who has opted out of the sale of the consumer's
5 personal information, respect the consumer's decision to opt out for at
6 least twelve months before requesting that the consumer authorize the
7 sale of the consumer's personal information; and

8 (6) Use any personal information collected from the consumer in
9 connection with the submission of the consumer's opt out request solely
10 for the purposes of complying with the opt out request.

11 (b) A consumer may authorize another person to opt out on the consum-
12 er's behalf, and a business shall comply with an opt out request
13 received from a person authorized by the consumer to act on the consum-
14 er's behalf.

15 8. (a) The obligations imposed on businesses by subdivisions two and
16 seven of this section shall not restrict a business's ability to:

17 (1) comply with federal, state, or local laws;

18 (2) comply with a civil, criminal, or regulatory investigation or
19 subpoena or summons by federal, state, or local authorities;

20 (3) cooperate with law enforcement agencies concerning conduct or
21 activity that the business reasonably and in good faith believes may
22 violate federal, state, or local law; or

23 (4) collect and sell a consumer's personal information if every aspect
24 of such commercial conduct takes place wholly outside of the state. For
25 purposes of this section, commercial conduct takes place wholly outside
26 of the state if the business collected such information while the
27 consumer was outside of the state, no part of the sale of the consumer's
28 personal information occurred in the state, and no personal information
29 collected while the consumer was in the state is sold.

30 (b) The obligations imposed on businesses by subdivisions two and
31 seven of this section shall not apply where compliance by the business
32 with this section would violate an evidentiary privilege under state law
33 and shall not prevent a business from providing the personal information
34 of a consumer to a person covered by an evidentiary privilege under
35 state law as part of a privileged communication.

36 (c) This section shall not apply to protected health information that
37 is collected by a covered entity governed by the medical privacy and
38 security rules issued by the Federal Department of Health and Human
39 Services, Parts 160 and 164 of Title 45 of the Code of Federal Regu-
40 lations, established pursuant to the Health Insurance Portability and
41 Availability Act of 1996 (HIPAA). For purposes of this subdivision, the
42 definitions of "protected health information" and "covered entity" from
43 the federal privacy rule shall apply.

44 (d) This section shall not apply to the sale of personal information
45 to or from a consumer reporting agency if that information is to be
46 reported in, or used to generate, a consumer report as defined by subdi-
47 vision (d) of Section 1681(a) of Title 15 of the United States Code, and
48 use of that information is limited by the federal Fair Credit Reporting
49 Act, 15 U.S.C. § 1681, et seq.

50 9. (a) A consumer who has suffered a violation of this section may
51 bring an action for statutory damages. A violation of this section shall
52 be deemed to constitute an injury in fact to the consumer who has
53 suffered the violation, and the consumer need not suffer a loss of money
54 or property as a result of the violation in order to bring an action for
55 a violation of this section.

1 (b)(1) Any consumer who suffers an injury in fact, as described in
2 paragraph (a) of this subdivision, shall recover statutory damages in
3 the amount of one thousand dollars or actual damages, whichever is
4 greater, for each violation from the business or person responsible for
5 the violation, except that in the case of a knowing and willful
6 violation by a business or person, an individual shall recover statutory
7 damages of not less than one thousand dollars and not more than three
8 thousand dollars, or actual damages, whichever is greater, for each
9 violation from the business or person responsible for the violation.

10 (2) In assessing the amount of statutory damages, the court shall
11 consider any one or more of the relevant circumstances presented by any
12 of the parties to the case, including, but not limited to, the follow-
13 ing: the nature and seriousness of the misconduct, the number of
14 violations, the persistence of the misconduct, the length of time over
15 which the misconduct occurred, the willfulness of the defendant's
16 misconduct, and the defendant's assets, liabilities, and net worth.

17 (c) Notwithstanding any other law, whenever a judgment, including any
18 consent judgment, decree, or settlement agreement, is approved by the
19 court in a class action based on a violation of this section, any cy
20 pres award, unpaid cash residue, or unclaimed or abandoned class member
21 funds attributable to a violation of this section shall be distributed
22 exclusively to one or more nonprofit organizations to support projects
23 that will benefit the class or similarly situated persons, further the
24 objectives and purposes of the underlying class action or cause of
25 action, or promote the law consistent with the objectives and purposes
26 of the underlying class action or cause of action, unless for good cause
27 shown the court makes a specific finding that an alternative distrib-
28 ution would better serve the public interest or the interests of the
29 class. If not specified in the judgment, the court shall set a date when
30 the parties shall submit a report to the court regarding a plan for the
31 distribution of any moneys pursuant to this subdivision.

32 (d) The remedies provided by this subdivision are cumulative to each
33 other and to the remedies or penalties available under all other laws of
34 the state.

35 10. (a) Any business or person that violates this section shall be
36 liable for a civil penalty in a civil action brought in the name of the
37 people of the state of New York by the attorney general.

38 (b) Notwithstanding any other law to the contrary, any person or busi-
39 ness that intentionally violates this section may be liable for a civil
40 penalty of up to seven thousand five hundred dollars for each violation.

41 (c) Notwithstanding any other law to the contrary, any civil penalty
42 assessed for a violation of this section, and the proceeds of any
43 settlement of an action brought pursuant to paragraph (a) of this subdi-
44 vision, shall be allocated as follows:

45 (1) twenty percent to the consumer privacy fund, created pursuant to
46 section ninety-nine-m of the state finance law, with the intent to fully
47 offset any costs incurred by the state courts and the attorney general
48 in connection with this section; and

49 (2) eighty percent to the jurisdiction on whose behalf the action
50 leading to the civil penalty was brought.

51 (d) The legislature shall adjust the percentages specified in para-
52 graph (c) of this subdivision and in subdivision eleven of this section,
53 as necessary to ensure that any civil penalties assessed for a violation
54 of this section fully offset any costs incurred by the state courts and
55 the attorney general in connection with this section, including a suffi-
56 cient amount to cover any deficit from a prior fiscal year. The legisla-

ture shall not direct a greater percentage of assessed civil penalties to the consumer privacy fund than reasonably necessary to fully offset any costs incurred by the state courts and the attorney general in connection with this section.

11. (a) Any person who becomes aware, based on non-public information, that a person or business has violated this section may file a civil action for civil penalties pursuant to subdivision ten of this section, if prior to filing such action, the person files with the attorney general a written request for the attorney general to commence the action. The request shall include a clear and concise statement of the grounds for believing a cause of action exists. The person shall make the non-public information available to the attorney general upon request.

(1) If the attorney general files suit within ninety days from receipt of the written request to commence the action, no other action may be brought unless the action brought by the attorney general is dismissed without prejudice.

(2) If the attorney general does not file suit within ninety days from receipt of the written request to commence the action, the person requesting the action may proceed to file a civil action.

(3) The time period within which a civil action shall be commenced shall be tolled from the date of receipt by the attorney general of the written request to either the date that the civil action is dismissed without prejudice, or for one hundred fifty days, whichever is later, but only for a civil action brought by the person who requested the attorney general to commence the action.

(b) Notwithstanding paragraph (c) of subdivision ten of this section, if a judgment is entered against the defendant or defendants in an action brought pursuant to this subdivision, or the matter is settled, amounts received as civil penalties or pursuant to a settlement of the action shall be allocated as follows:

(1) If the action was brought by the attorney general upon a request made by a person pursuant to paragraph (a) of this subdivision, the person who made the request shall be entitled to fifteen percent of the civil penalties, and the remaining proceeds shall be deposited in the consumer privacy fund pursuant to section ninety-nine-m of the state finance law.

(2) If the action was brought by the person who made the request pursuant to paragraph (a) of this subdivision, that person shall receive an amount the court determines is reasonable for collecting the civil penalties on behalf of the government. The amount shall be not less than twenty-five percent and not more than fifty percent of the proceeds of the action and shall be paid out of the proceeds. The remaining proceeds shall be deposited in the consumer privacy fund pursuant to section ninety-nine-m of the state finance law.

(c) For purposes of this section, "non-public information" means information that has not been disclosed in a criminal, civil, or administrative proceeding, in a government investigation, report, or audit, or by the news media or other public source of information, and that was not obtained in violation of the law.

12. A business that suffers a breach of the security of the system involving consumers' personal information shall be deemed to have violated this section and may be held liable for such violation or violations under subdivisions nine, ten and eleven of this section, if the business has failed to implement and maintain reasonable security

1 procedures and practices, appropriate to the nature of the information,
2 to protect the personal information from unauthorized disclosure.

3 13. This section is intended to further the constitutional right of
4 privacy and to supplement existing laws relating to consumers' personal
5 information. The provisions of this section are not limited to informa-
6 tion collected electronically or over the internet, but apply to the
7 collection and sale of all personal information collected by a business
8 from consumers. Wherever possible, existing law relating to consumers'
9 personal information should be construed to harmonize with the
10 provisions of this section, but in the event of conflict between exist-
11 ing law and the provisions of this section, the provisions of the law
12 that afford the greatest protection for the right of privacy for consum-
13 ers shall control.

14 14. Nothing in this section shall prevent a city, county, city and
15 county, municipality, or local agency from safeguarding the constitu-
16 tional right of privacy by imposing additional requirements on busi-
17 nesses regarding the collection and sale of consumers' personal informa-
18 tion by businesses provided that the requirement does not prevent a
19 person or business from complying with this section.

20 15. (a) The attorney general shall adopt regulations in the following
21 areas to further the purposes of this section:

22 (1) Adding additional categories to those enumerated in paragraph (c)
23 of subdivision six and paragraph (m) of subdivision one of this section
24 in order to address changes in technology, data collection practices,
25 obstacles to implementation, and privacy concerns. In addition, upon
26 receipt of a request made by a city attorney or district attorney to add
27 a new category or categories, the attorney general shall promulgate a
28 regulation to add such category or categories unless the attorney gener-
29 al concludes, based on factual or legal findings, that there is a
30 compelling reason not to add the category or categories. The attorney
31 general may also add additional categories to those enumerated in para-
32 graph (c) of subdivision six and paragraph (m) of subdivision one of
33 this section in response to a petition filed;

34 (2) Adding additional items to the definition of "unique identifiers"
35 to address changes in technology, data collection, obstacles to imple-
36 mentation, and privacy concerns, and additional categories to the defi-
37 nition of "designated methods for submitting requests" to facilitate a
38 consumer's ability to obtain information from a business pursuant to
39 subdivision six of this section;

40 (3) Establishing any exceptions necessary to comply with state or
41 federal law;

42 (4) Establishing rules and procedures: (A) to facilitate and govern
43 the submission of a request by a consumer, and by an authorized agent of
44 the consumer, to opt out of the sale of personal information pursuant to
45 subparagraph one of paragraph (a) of subdivision seven of this section;
46 (B) to govern a business's compliance with a consumer's opt out request;
47 and (C) for the development and use of a recognizable and uniform opt
48 out logo or button by all businesses to promote consumer awareness of
49 the opportunity to opt out of the sale of personal information;

50 (5) Adjusting the monetary threshold in clause (A) of subparagraph one
51 of paragraph (b) of subdivision one of this section in January of every
52 odd-numbered year to reflect any increase in the Consumer Price Index;

53 (6) Establishing rules, procedures, and any exceptions necessary to
54 ensure that the notices and information that businesses are required to
55 provide pursuant to this section are provided in a manner so as to be
56 easily understood by the average consumer, are accessible to consumers

1 with disabilities, and are available in the language primarily used to
2 interact with the consumer;

3 (7) Establishing rules and procedures to further the purposes of
4 subdivisions two and three of this section and to facilitate a consum-
5 er's or the consumer's authorized agent's ability to obtain information
6 pursuant to subdivision six of this section, with the goal of minimizing
7 the administrative burden on consumers, taking into account available
8 technology, security concerns, and the burden on the business, to govern
9 a business's determination that a request for information received by a
10 consumer is a verifiable request, including treating a request submitted
11 through a password protected account maintained by the consumer with the
12 business while the consumer is logged into the account as a verifiable
13 request and providing a mechanism for a consumer who does not maintain
14 an account with the business to request information through the busi-
15 ness's authentication of the consumer's identity;

16 (8) Defining the term "valuable consideration" as used in subparagraph
17 one of paragraph (q) of subdivision one of this section to ensure that a
18 business that discloses, except as permitted by this section, a consum-
19 er's personal information to a third party, including through a series
20 of transactions involving multiple third parties, in exchange for any
21 economic benefit is subject to this section, and to include business
22 practices involving the disclosure of personal information in exchange
23 for something of value. Valuable consideration does not include the
24 exchange of value in a transaction involving non-commercial speech, such
25 as journalism and political speech; and

26 (9) Further interpret the terms "de-identified", "sell", "third
27 party", and "business purpose" as set forth in subdivision one of this
28 section, to address changes in technology, data collection, obstacles to
29 implementation, and privacy concerns and to ensure compliance with the
30 purposes of this section, provided that such regulations do not reduce
31 consumer privacy or the ability of consumers to stop the sale of their
32 personal information.

33 (b) The attorney general shall be precluded from adopting regulations
34 that limit or reduce the number or scope of categories of personal
35 information enumerated in paragraph (c) of subdivision six and paragraph
36 (m) of subdivision one of this section, or that limit or reduce the
37 number or scope of categories added pursuant to subparagraph one of
38 paragraph (a) of this subdivision, except as necessary to comply with
39 subparagraph three of paragraph (a) of this subdivision. The attorney
40 general shall also be precluded from reducing the scope of the defi-
41 nition of "unique identifiers", except as necessary to comply with
42 subparagraph three of paragraph (a) of this subdivision.

43 (c) To the extent the attorney general determines that it is necessary
44 to adopt certain regulations in order to implement this section, the
45 attorney general shall adopt any such regulations within six months of
46 the date this section is adopted.

47 (d) The attorney general may adopt additional regulations as necessary
48 to further the purposes of this section.

49 16. If a series of steps or transactions were component parts of a
50 single transaction intended from the beginning to be taken with the
51 intention of avoiding the reach of this section, including the disclo-
52 sure of information by a business to a third party in order to avoid the
53 definition of "sell", a court shall disregard the intermediate steps or
54 transactions for purposes of effectuating the purposes of this section.

55 17. Any provision of a contract or agreement of any kind that purports
56 to waive or limit in any way a consumer's rights under this section,

1 including but not limited to any right to a remedy or means of enforce-
2 ment, shall be deemed contrary to public policy and shall be void and
3 unenforceable. This section shall not prevent a consumer from: declin-
4 ing to request information from a business; declining to opt out of a
5 business's sale of the consumer's personal information; or authorizing a
6 business to sell the consumer's personal information after previously
7 opting out.

8 18. If any provision of this section shall be adjudged by any court of
9 competent jurisdiction to be invalid, such judgment shall not affect,
10 impair or invalidate the remainder thereof, but shall be confined in its
11 operation to the provision directly involved in the controversy in which
12 such judgment shall have been rendered.

13 § 3. The state finance law is amended by adding a new section 99-m to
14 read as follows:

15 § 99-m. Consumer privacy fund. 1. There is hereby established in the
16 joint custody of the state comptroller and the commissioner of taxation
17 and finance an account within the general fund to be known as the
18 "consumer privacy fund".

19 2. Such account shall consist of all penalties received by the depart-
20 ment of state pursuant to section eight hundred ninety-nine-cc of the
21 general business law and any additional monies appropriated, credited or
22 transferred to such account by the legislature. Any interest earned by
23 the investment of monies in such account shall be added to such account,
24 become part of such account, and be used for the purposes of such
25 account.

26 3. Monies in the account shall be available to the office of court
27 administration and the attorney general to offset any costs incurred by
28 the state courts in connection with actions brought to enforce section
29 eight hundred ninety-nine-cc of the general business law and any costs
30 incurred by the attorney general in carrying out his or her duties under
31 such section of law.

32 4. Monies in the account shall be paid out of the account on the audit
33 and warrant of the state comptroller on vouchers certified or approved
34 by the office of court administration and/or the attorney general.

35 § 4. This act shall take effect on the one hundred eightieth day after
36 it shall have become a law. Effective immediately, the addition, amend-
37 ment and/or repeal of any rule or regulation necessary for the implemen-
38 tation of this act on its effective date are authorized to be made and
39 completed on or before such effective date.