[Third Reprint]
ASSEMBLY, No. 1971

STATE OF NEW JERSEY

220th LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2022 SESSION

Sponsored by:
Assemblyman RAJ MUKHERJI
District 33 (Hudson)
Assemblyman DANIEL R. BENSON
District 14 (Mercer and Middlesex)
Assemblyman PAUL D. MORIARTY
District 4 (Camden and Gloucester)
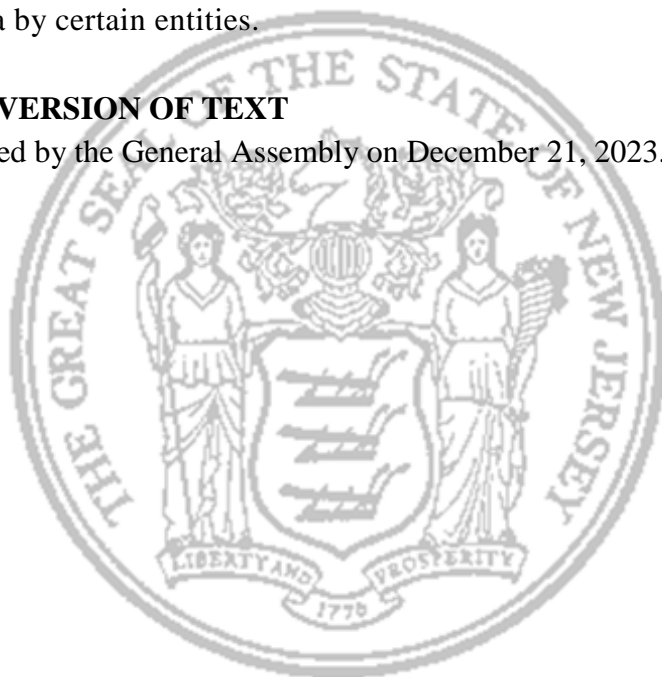
Co-Sponsored by:
Assemblywoman McKnight, Assemblymen DeAngelo, Verrelli and Wimberly

SYNOPSIS
    Requires notification to consumers of collection and disclosure of personal data by certain entities.

CURRENT VERSION OF TEXT
    As amended by the General Assembly on December 21, 2023.

(Sponsorship Updated As Of: 12/14/2023)

1   **AN ACT** concerning **¹[**commercial Internet websites**]** <u>online</u>
2   <u>services</u>**¹** , consumers, and **²[**personally identifiable information**]**
3   <u>personal data</u>**²** and supplementing Title 56 of the Revised
4   Statutes.

5

6   **BE IT ENACTED** *by the Senate and General Assembly of the State*
7   *of New Jersey:*

8

9   1. As used in P.L.   , c.   (C.   ) (pending before the
10 Legislature as this bill):
11 "Affiliate" means a legal entity that controls, is controlled by, or
12 is under common control with another legal entity **²**<u>. For the</u>
13 <u>purposes of this definition, "control" means: the ownership of, or</u>
14 <u>the power to vote, more than 50 percent of the outstanding shares of</u>
15 <u>any class of voting security of a company; the control in any</u>
16 <u>manner over the election of a majority of the directors or</u>
17 <u>individuals exercising similar functions; or the power to exercise a</u>
18 <u>controlling influence over the management or policies of a</u>
19 <u>company</u>**²**.
20   **²[¹**<u>"Business" means a sole proprietorship, partnership, limited</u>
21 <u>liability company, corporation, association, or other legal entity that</u>
22 <u>is organized or operated for the profit or financial benefit of its</u>
23 <u>shareholders or other owners, that collects consumers' personal</u>
24 <u>information. "Business" does not include non-profit</u>
25 <u>organizations.</u>**¹]²**
26   **¹[**"Commercial Internet website" means a website operated for
27 business purposes, including, but not limited to, the sale of goods
28 and services, which collects and maintains personally identifiable
29 information from a consumer.**]¹**
30   **²**<u>"Biometric data" means data generated by automatic or</u>
31 <u>technological processing, measurements, or analysis of an</u>
32 <u>individual's biological, physical, or behavioral characteristics,</u>
33 <u>including, but not limited to, fingerprint, voiceprint, eye retinas,</u>
34 <u>irises, facial mapping, facial geometry, facial templates, or other</u>
35 <u>unique biological, physical, or behavioral patterns or characteristics</u>
36 <u>that are used or intended to be used, singularly or in combination</u>
37 <u>with each other or with other personal data, to identify a specific</u>
38 <u>individual. "Biometric data" shall not include: a digital or physical</u>
39 <u>photograph; an audio or video recording; or any data generated</u>
40 <u>from a digital or physical photograph, or an audio or video</u>
41 <u>recording, unless such data is generated to identify a specific</u>
42 <u>individual.</u>

1   "Child" shall have the same meaning as provided in COPPA.

2   "Consent" means a clear affirmative act signifying a consumer's
3   freely given, specific, informed and unambiguous agreement to
4   allow the processing of personal data relating to the consumer.
5   "Consent" may include a written statement, including by electronic
6   means, or any other unambiguous affirmative action. "Consent shall
7   not include: acceptance of a general or broad terms of use or similar
8   document that contains descriptions of personal data processing
9   along with other, unrelated information; hovering over, muting,
10   pausing, or closing a given piece of content; or agreement obtained
11   through the use of dark patterns.**2**

12   "Consumer" means an identified person who is a resident of this
13   State acting only in an individual or household context. "Consumer"
14   shall not include a person acting in a commercial or employment
15   context.

16   **2**"Controller" means an individual or legal entity that, alone or
17   jointly with others, determines the purpose and means of processing
18   personal data.

19   "COPPA" means the federal Children's Online Privacy
20   Protection Act, 15 U.S.C. s.6501 et seq., and any rules, regulations,
21   guidelines, and exceptions thereto, as may be amended from time to
22   time.

23   "Dark pattern" means a user interface designed or manipulated
24   with the substantial effect of subverting or impairing user
25   autonomy, decision-making, or choice, and includes, but is not
26   limited to, any practice the United States Federal Trade
27   Commission refers to as a "dark pattern."

28   "Decisions that produce legal or similarly significant effects
29   concerning the consumer" means decisions that result in the
30   provision or denial of financial or lending services, housing,
31   insurance, education enrollment or opportunity, criminal justice,
32   employment opportunities, health care services, or access to
33   essential goods and services.**2**

34   "De-identified data" means: data that cannot be **2**reasonably used
35   to infer information about, or otherwise be**2** linked to **2**[a consumer
36   without additional information that is kept separately; or data that
37   has been modified to a degree that the risk of re-identification,
38   consistent with guidance from the Federal Trade Commission and
39   the National Institute of Standards and Technology, is small, as
40   determined by the Director of the Division of Consumer Affairs in
41   the Department of Law and Public Safety pursuant to section **1**[8]
42   9**1**of P.L.   , c.   (C.   ) (pending before the Legislature as this
43   bill), that is subject to a public commitment by the operator] an
44   identified or **3**[reasonably]**3** identifiable individual, or a device
45   linked to such an individual, if the controller that possesses the
46   data: (1) takes reasonable measures to ensure that the data cannot be
47   associated with an individual, (2) publicly commits to maintain and

1   <u>use the data only in a de-identified fashion and</u>**²** not to attempt to re-

2   identify the data, and **²[**to which one or more enforceable controls

3   to prevent re-identification has been applied, which may include

4   legal, administrative, technical, or contractual controls**]** <u>(3)</u>

5   <u>contractually obligates any recipients of the information to comply</u>

6   <u>with the requirements of this paragraph</u>**²**.

7   "Designated request address" means an electronic mail address,

8   Internet website, or toll-free telephone number that a consumer may

9   use to request the information required to be provided pursuant to

10   section 3 of P.L.   , c.   (C.   ) (pending before the Legislature as

11   this bill).

12   **²[**"Disclose" means to release, transfer, share, disseminate, make

13   available, or otherwise communicate orally, in writing, or by

14   electronic or any other means **¹**<u>by an operator</u>**¹** to a third party a

15   consumer's personally identifiable information. "Disclose" shall not

16   include:

17   the disclosure of a consumer's personally identifiable

18   information by an operator to a third party under a written contract

19   authorizing the third party to use the personally identifiable

20   information to perform services on behalf of the operator, including

21   maintaining or servicing accounts, providing customer service,

22   processing or fulfilling orders and transactions, verifying consumer

23   information, processing payments, providing financing, or similar

24   services, but only if the contract prohibits the third party from using

25   the personally identifiable information for any reason other than

26   performing the specified service on behalf of the operator and from

27   disclosing personally identifiable information to additional third

28   parties unless expressly authorized by the consumer;

29   the disclosure of personally identifiable information by an

30   operator to a third party based on a good-faith belief that disclosure

31   is required to comply with **¹**<u>an</u>**¹** applicable law, regulation, legal

32   process, or court order;

33   the disclosure of personally identifiable information by an

34   operator to a third party that is reasonably necessary to address

35   fraud, risk management, security, or technical issues, to protect the

36   operator's rights or property, or to protect a consumer or the public

37   from illegal activities as required by law; or

38   the disclosure of personally identifiable information by an

39   operator to a third party in connection with the proposed or actual

40   sale or merger of the operator, or sale of all or part of its assets, to a

41   third party.

42   "Online service" means **¹[**an information**]** <u>any</u>**¹** service provided

43   over the Internet that collects and maintains personally identifiable

44   information from a consumer.

45   "Operator" means a person or entity that operates **¹[**a

46   commercial Internet website or**]¹** an online service. "Operator"

47   shall not include any third party that operates, hosts, or manages,

1   but does not own, **1**[a commercial Internet website or] <u>an</u>**1** online
2   service on the operator's behalf, or processes information on behalf
3   of the operator.
4   "Personally identifiable information"] <u>"Personal data"</u>**2** means
5   any information that is linked or reasonably linkable to an identified
6   or identifiable person. "**2**[Personally identifiable information]
7   <u>Personal data</u>**2**" shall not include de-identified data or publicly
8   available information.
9   **2**<u>"Precise geolocation data" means information derived from</u>
10   <u>technology, including, but not limited to, global positioning system</u>
11   <u>level latitude and longitude coordinates or other mechanisms, that</u>
12   <u>directly identifies the specific location of an individual with</u>
13   <u>precision and accuracy within a radius of 1,750 feet. "Precise</u>
14   <u>geolocation data" does not include the content of communications,</u>
15   <u>or any data generated by or connected to advanced utility metering</u>
16   <u>infrastructure systems or equipment for use by a utility.</u>
17   <u>"Process" or "processing" means an operation or set of</u>
18   <u>operations performed, whether by manual or automated means, on</u>
19   <u>personal data or on sets of personal data, such as the collection, use,</u>
20   <u>storage, disclosure, analysis, deletion, or modification of personal</u>
21   <u>data, and also includes the actions of a controller directing a</u>
22   <u>processor to process personal data.</u>
23   <u>"Processor" means a person, private entity, public entity, agency,</u>
24   <u>or other entity that processes personal data on behalf of the</u>
25   <u>controller.</u>
26   <u>"Profiling" means any form of automated processing performed</u>
27   <u>on personal data to evaluate, analyze or predict personal aspects</u>
28   <u>related to an identified or identifiable individual's economic</u>
29   <u>situation, health, personal preferences, interests, reliability,</u>
30   <u>behavior, location or movements.</u>**2**
31   "Publicly available information" means information that is
32   lawfully made available from federal, State, or local government
33   records, or widely-distributed media **2**<u>or information that a</u>
34   <u>controller has a reasonable basis to believe a consumer has lawfully</u>
35   <u>made available to the general public and has not restricted to a</u>
36   <u>specific audience</u>**2**.
37   "Sale" means **2**[the exchange of personally identifiable
38   information for monetary consideration by the operator to a third
39   party for purposes of licensing or selling personally identifiable
40   information at the third party's discretion to additional third parties.
41   "Sale" shall not include the following:
42   the disclosure of personally identifiable information to a service
43   provider that processes that information on behalf of the operator;
44   the disclosure of personally identifiable information to a third
45   party with whom the consumer has a direct relationship for
46   purposes of providing a product or service requested by the
47   consumer or otherwise in a manner that is consistent with a

1 consumer's reasonable expectations considering the context in
2 which the consumer provided the personally identifiable
3 information to the operator;
4   the disclosure or transfer of personally identifiable information
5 to an affiliate of the operator; or
6   the disclosure or transfer of personally identifiable information
7 to a third party as an asset that is part of a merger, acquisition,
8 bankruptcy, or other transaction in which the third party assumes
9 control of all or part of the operator's assets**]** the sharing,
10 disclosing, or transferring of personal data for monetary or other
11 valuable consideration by the controller to a third party. "Sale" shall
12 not include:
13   The disclosure of personal data to a processor that **[3[**only**]3**
14 processes the personal data on the controller's behalf;
15   The disclosure of personal data to a third party for the purposes
16 of providing a product or service requested by the consumer;
17   The disclosure or transfer of personal data to an affiliate of the
18 controller;
19   The disclosure of personal data that the consumer intentionally
20 made available to the general public through a mass media channel
21 and did not restrict to a specific audience; or
22   The disclosure or transfer of personal data to a third party as an
23 asset that is part of a proposed or actual merger, acquisition,
24 bankruptcy, or other transaction in which the third party assumes
25 control of all or part of the controller's assets[2].
26   **[2[**"Service provider" means a person, private entity, public
27 entity, agency, or other entity that processes personally identifiable
28 information on behalf of the operator and who shall provide
29 sufficient guarantees to the operator to implement appropriate
30 technical and organizational measures in a manner that processing
31 shall ensure the protection of the consumer's personally identifiable
32 information**]**
33   "Sensitive data" means personal data revealing racial or ethnic
34 origin; religious beliefs; mental or physical health condition,
35 treatment, or diagnosis; financial information [3], which shall include
36 a consumer's account number, account log-in, financial account, or
37 credit or debit card number, in combination with any required
38 security code, access code, or password that would permit access to
39 a consumer's financial account[3] ; sex life or sexual orientation;
40 citizenship or immigration status; status as transgender or non-
41 binary; genetic or biometric data that may be processed for the
42 purpose of uniquely identifying an individual; personal data
43 collected from a known child; or precise geolocation data.
44   "Targeted advertising" means displaying **[3[**an**]3** advertisements
45 to a consumer where the advertisement is selected based on
46 personal data obtained or inferred from that consumer's activities
47 over time and across nonaffiliated Internet web sites or online

1   applications to predict such consumer's preferences or interests.
2   "Targeted advertising" shall not include: advertisements based on
3   activities within a controller's own internet websites or online
4   applications; advertisements based on the context of a consumer's
5   current search query, visit to an internet website or online
6   application; advertisements directed to a consumer in response to
7   the consumer's request for information or feedback; or processing
8   personal data solely to measure or report advertising frequency,
9   performance, or reach**²**.
10   "Third party" means a person, private entity, public entity,
11   agency, or entity other than the consumer, **²[**operator**]** controller**²**,
12   or affiliate or **²[**service provider**]** processor**²** of the **²[**operator**]**
13   controller**²**.
14   **²**"Trade secret" has the same meaning as section 2 of P.L.2011,
15   c.161 (C.56:15-2).**²**
16   "Verified request" means the process through which a consumer
17   may submit a request to exercise a right or rights established in
18   P.L.   , c.   (C.   ) (pending before the Legislature as this bill),
19   and by which **²[**an operator**]** a controller**²** can reasonably
20   authenticate the request and the consumer making the request using
21   commercially reasonable means.
22
23   **²**2. Notwithstanding any State law, rule, regulation, or order to
24   the contrary, the provisions of P.L.   , c.   (C.   ) (pending
25   before the Legislature as this bill) shall only apply to controllers
26   that conduct business in the State or produce products or services
27   that are targeted to residents of the State, and that during a calendar
28   year either:
29   a. control or process the personal data of at least 100,000
30   consumers, excluding personal data processed solely for the
31   purpose of completing a payment transaction; or
32   b. control or process the personal data of at least 25,000
33   consumers and the controller derives revenue, or receives a discount
34   on the price of any goods or services, from the sale of personal
35   data.**²**
36
37   **²[**2**]** 3**²**.   a.   **²[**An operator that collects the personally
38   identifiable information of a consumer through **¹[**a commercial
39   Internet website or**]** an**¹** online service**]** A controller**²** shall provide
40   **²[**on **¹[**its commercial Internet website or**]** the**¹** online service
41   notification**]²** to a consumer **²**a reasonably accessible, clear, and
42   meaningful privacy notice**²** that shall include, but **²**may**²** not be
43   limited to:
44   (1) the categories of the **²[**personally identifiable information**]**
45   personal data**²** that the **²[**operator collects through the
46   **¹[**commercial Internet website or **]¹** online service about a

1   consumer who uses or visits the operator's **¹[**commercial Internet
2   website or**]¹** online service**]** <u>controller processes</u>**²**;
3   (2) **²**<u>the purpose for processing personal data;</u>
4   <u>(3)</u>**²** the categories of all third parties **¹[**with**]** <u>to</u>**¹** which the
5   **²[**operator**]** <u>controller</u>**²** may disclose a consumer's **²[**personally
6   identifiable information**]** <u>personal data</u>**²**;
7   **²[**(3)   whether a third party may collect personally
8   identifiable information about a consumer's online activities over
9   time and across different **¹[**commercial Internet websites or **]¹**
10 online services when the consumer uses the **¹[**Internet website or**]¹**
11 online service of the operator;
12   (4) a description of the process for an individual consumer who
13 uses or visits the **¹[**commercial Internet website or **]¹** online service
14 to review and request changes to any of the consumer's personally
15 identifiable information that is collected by the **¹[**commercial
16 Internet website or **]¹** online service of the operator;
17   (5)**]** <u>(4) the categories of personal data that the controller shares</u>
18 <u>with third parties, if any;</u>
19   <u>(5) how consumers may exercise their consumer rights, including</u>
20 <u>the controller's contact information and how a consumer may</u>
21 <u>appeal a controller's decision with regard to the consumer's</u>
22 <u>request;</u>
23   <u>(6)</u>**²** the process by which the **²[**operator**]** <u>controller</u>**²** notifies
24 consumers **²[**who use or visit the **¹[**commercial Internet website
25 or**]¹** online service**]²** of material changes to the notification
26 required to be made available pursuant to this subsection, along
27 with the effective date of the notice; and
28   **²[**(6) information concerning one or more designated request
29 addresses of the operator.
30   b.   In addition to the requirements of subsection a. of this
31 section, an operator shall include the notification as a separate
32 section of the operator's privacy policy**]** **³[**<u>; and</u>**]³**
33   <u>(7) an active electronic mail address or other online mechanism</u>
34 <u>that the consumer may use to contact the controller.</u>
35   <u>b. If a controller sells personal data to third parties or processes</u>
36 <u>personal data for the purposes of targeted advertising, the sale of</u>
37 <u>personal data, or profiling in furtherance of decisions that produce</u>
38 <u>legal or similarly significant effects concerning a consumer, the</u>
39 <u>controller shall clearly and conspicuously disclose such sale or</u>
40 <u>processing, as well as the manner in which a consumer may</u>
41 <u>exercise the right to opt out of such sale or processing</u> **³[**<u>, a</u>
42 <u>description of the process for a consumer to review and make</u>
43 <u>requests pursuant to section 4 of this act, P.L.   , c.   (C.   )</u>
44 <u>(pending before the Legislature as this bill)</u>**]³**<u>.</u>
45   <u>c.   A controller shall not:</u>

1 (1) require a consumer to create a new account in order to
2 exercise a right **3**, but may require a consumer to use an existing
3 account to submit a verified request**3** ; or
4 (2) based solely on the exercise of a right and unrelated to
5 feasibility or the value of a service, increase the cost of, or decrease
6 the availability of, the product or service.**2**
7
8 **2**[3. a. An operator that collects a consumer's personally
9 identifiable information through its **1**[commercial Internet website
10 or]**1** online service and discloses the consumer's personally
11 identifiable information to a third party shall make the following
12 information available to the consumer free of charge upon receipt of
13 a verified request from the consumer for this information through a
14 designated request address:
15 (1) the category or categories of a consumer's personally
16 identifiable information that were disclosed; and
17 (2) the category or categories of the third parties that received
18 the consumer's personally identifiable information.
19 b. An operator] 4. a. A controller**2** that receives a verified
20 request from a consumer **2**[pursuant to subsection a. of this
21 section]**2** shall provide a response to the consumer within **2**[60] 45**2**
22 days of the **2**[operator's verification] controller's reciept**2** of the
23 request **2**. The controller may extend the response period by 45
24 additional days where reasonably necessary, considering the
25 complexity and number of the consumer's requests, provided that
26 the controller informs the consumer of any such extension within
27 the initial 45-day response period and the reason for the extension**2**
28 and shall provide the information**2**[, pursuant to subsection a. of
29 this section,]**2** for all disclosures of **2**[personally identifiable
30 information] personal data**2** that occurred in the prior 12 months.
31 **2**[c. This section shall not apply to personally identifiable
32 information disclosed prior to the effective date of
33 P.L.   , c. (C.   ) (pending before the Legislature as this bill)]
34 b**2**. **1**This section shall not apply to **2**[personally identifiable
35 information] personal data**2** collected prior to the effective date of
36 P.L.   , c. (C.   ) (pending before the Legislature as this bill)
37 unless the controller continues to **2**[store] process**2** such
38 information thereafter.**1**
39 **2**c. If a controller declines to take action regarding the
40 consumer's request, the controller shall inform the consumer
41 without undue delay, but not later than 45 days after receipt of the
42 request, of the justification for declining to take action and
43 instructions for how to appeal the decision.
44 d. Information provided in response to a consumer request shall
45 be provided by a controller, free of charge, once per consumer
46 during any twelve-month period **3**[, except that, for a second or

1   subsequent identical request within a 12-month period, the
2   controller may charge an amount calculated pursuant to
3   regulations**]³**.   If requests from a consumer are manifestly
4   unfounded, excessive, or repetitive, the controller may charge the
5   consumer a reasonable fee to cover the administrative costs of
6   complying with the request or decline to act on the request. The
7   controller shall bear the burden of demonstrating the manifestly
8   unfounded, excessive or repetitive nature of the request.
9   e. If a controller is unable to authenticate a request to exercise
10 any of the rights afforded under section 5 of P.L.   , c.   (C.   )
11 (pending before the Legislature as this bill) using commercially
12 reasonable efforts, the controller shall not be required to comply
13 with a request to initiate an action pursuant to this section and shall
14 provide notice to the consumer that the controller is unable to
15 authenticate the request to exercise such right or rights until such
16 consumer provides additional information reasonably necessary to
17 authenticate such consumer and such consumer's request to exercise
18 such right or rights. A controller shall not be required to
19 authenticate an opt-out request **³[**it honors**]³**, but a controller may
20 deny an opt-out request if the controller has a good faith, reasonable
21 and documented belief that such request is fraudulent. If a
22 controller denies an opt-out request because the controller believes
23 such request is fraudulent, the controller shall send a notice to the
24 person who made such request disclosing that such controller
25 believes such request is fraudulent, why such controller believes
26 such request is fraudulent and that such controller shall not comply
27 with such request.
28   f. A controller shall establish a process for a consumer to appeal
29 the controller's refusal to take action on a request within a
30 reasonable period of time after the consumer's receipt of the
31 decision. The appeal process shall be conspicuously available and
32 similar to the process for submitting requests to initiate action
33 pursuant to this section. Not later than 45 days after receipt of an
34 appeal, a controller shall inform the consumer in writing of any
35 action taken or not taken in response to the appeal, including a
36 written explanation of the reasons for the decisions. If the appeal is
37 denied, the controller shall also provide the consumer with an
38 online mechanism, if available, or other method through which the
39 consumer may contact the Division of Consumer Affairs in the
40 Department of Law and Public Safety to submit a complaint.**²**
41
42   **²[**4. a. An operator that collects the personally identifiable
43 information of a consumer through its **¹[**commercial Internet
44 website or**]¹** online service and sells the personally identifiable
45 information of the consumer **¹[**through the Internet**]¹** shall clearly
46 and conspicuously post a link, on its **¹[**commercial Internet website
47 or**]¹** online service or in another prominently accessible location the

1 **[1][**commercial Internet website**]** online service**[1]** maintains for
2 consumer privacy settings, to an Internet webpage maintained by
3 the operator, which enables a consumer, by verified request, to opt
4 **[1][**out of**]** into**[1]** the sale of the consumer's personally identifiable
5 information. The method in which a consumer may opt **[1][**out**]** in**[1]**
6 shall be in a form and manner determined by the operator, provided
7 that a consumer shall not be required to establish an account with
8 the operator in order to opt **[1][**out of**]** into**[1]** the sale of a consumer's
9 personally identifiable information.
10   b.   An operator**]** 5.   A controller**[2]** shall be prohibited from
11 discriminating against a consumer if the consumer chooses to opt
12 out of the **[2]**processing for**[2]** sale **[2]**, targeted advertising, or profiling
13 in furtherance of decisions that produce legal or similarly
14 significant effects**[2]** of the consumer's **[2][**personally identifiable
15 information pursuant to subsection a. of this section**]** personal data
16 pursuant to P.L.   , c.   (C.   ) (pending before the Legislature
17 as this bill)**[2]**. The provisions of this section shall not prohibit the
18 **[2][**operator's**]** controller's**[2]** ability to offer consumers discounts,
19 loyalty programs, or other incentives for the sale of the consumer's
20 **[2][**personally identifiable information**]** personal data**[2]**, or to provide
21 different services to consumers that are reasonably related to the
22 value of the relevant data **[1]**, provided that the **[2][**operator**]**
23 controller**[2]** has clearly and conspicuously disclosed to the consumer
24 that the offered discounts, programs, incentives, or services
25 **[2][**require consenting to**]** include**[2]** the sale or processing of
26 **[2][**personally identifiable information**]** personal data**[2]** that the
27 consumer otherwise has a right to opt out of**[1]**.
28
29   **[2][**5.**]** 6.**[2]** A waiver of the requirements of, or an agreement that
30 does not comply with, the provisions of P.L.   , c.   (C.   )
31 (pending before the Legislature as this bill) shall be void and
32 unenforceable.
33
34   **[2][**6. Nothing in P.L.   , c.   (C.   ) (pending before the
35 Legislature as this bill) shall apply to:
36   a.   protected health information collected by a covered entity or
37 business associate subject to the privacy, security, and breach
38 notification rules issued by the United States Department of Health
39 and Human Services, Parts 160 and 164 of Title 45 of the Code of
40 Federal Regulations, established pursuant to the "Health Insurance
41 Portability and Accountability Act of 1996," Pub.L.104-191, and
42 the "Health Information Technology for Economic and Clinical
43 Health Act," **[1][(]**[1]** 42 U.S.C. s.17921 et seq. **[1][)]**[1]**.
44   b.   a financial institution or an affiliate of a financial institution
45 that is subject to Title V of the federal "Gramm-Leach-Bliley Act

1   **¹[**of 1999**]¹** ,” 15 U.S.C. s.6801 et seq., and the rules and
2   implementing regulations promulgated thereunder;
3   c.   the   secondary   market   institutions   identified   in
4   15 U.S.C. s.6809(3)(D) and 12 C.F.R. s.1016.3(l)(3)(iii); **¹[**or**]¹**
5   d.   an   insurance   institution   subject   to   P.L.1985,   c.179
6   (C.17:23A-1 et seq.) **¹[**.**]** ;**¹**
7   e.   the sale of a consumer's personally identifiable information
8   by the New Jersey Motor Vehicle Commission that is permitted by
9   the federal "Drivers' Privacy Protection Act of 1994," 18 U.S.C.
10   s.2721 et seq.; **¹[**and**]** or**¹**
11   f.   personally identifiable information collected, processed,
12   sold, or disclosed by a consumer reporting agency, as defined in 15
13   U.S.C. s.1681a(f), if the collection, processing, sale, or disclosure
14   of the personally identifiable information is limited by the federal
15   "Fair   Credit   Reporting   Act,"   15   U.S.C.   s.1681   et   seq.,   and
16   implementing regulations.**]²**
17
18   **²[**7.   Nothing in P.L.   , c.   (C.   ) (pending before the
19   Legislature as this bill) shall require an operator to:
20   a.   re-identify de-identified data;
21   b.   collect, retain, use, link, or combine personally identifiable
22   information concerning a consumer that it would not otherwise
23   collect, retain, use, link, or combine in the ordinary course of
24   business.**]²**
25
26   **²[**8.   It shall be an unlawful practice and violation of P.L.1960,
27   c.39 (C.56:8-1 et seq.) for an operator to fail to notify a consumer of
28   the sale of personally identifiable information pursuant to sections 2
29   and 3 of P.L.   , c.   (C.   ) (pending before the Legislature as this
30   bill) or fail to allow a consumer to opt out of the sale of a
31   consumer's personally identifiable information pursuant to section 4
32   of P.L.   , c.   (C.   ) (pending before the Legislature as this bill)
33   if the operator fails to cure any alleged violation of
34   P.L.   , c.   (C.   ) (pending before the Legislature as this bill)
35   within 30 days after receiving notice of alleged noncompliance
36   from the Attorney General.**]²**
37
38   **²**7. a. A consumer shall have the right to:
39   (1) confirm whether a controller processes the consumer's
40   personal data and accesses such personal data, provided that
41   nothing in this paragraph shall require a controller to provide the
42   data to the consumer in a manner that would reveal the controller's
43   trade secrets;
44   (2) correct inaccuracies in the consumer's personal data, taking
45   into account the nature of the information and the purposes of the
46   processing of the information;
47   (3) delete personal data concerning the consumer;

1   (4) obtain a copy of the consumer's personal data held by the
2   controller in a portable and, to the extent technically feasible,
3   readily usable format that allows the consumer to transmit the data
4   to another entity without hindrance, provided that nothing in this
5   paragraph shall require a controller to provide the data to the
6   consumer in a manner that would reveal the controller's trade
7   secrets; and
8   (5) opt out of the processing of personal data for the purposes of
9   (a) targeted advertising; (b) the sale of personal data; or (c)
10   profiling in furtherance of decisions that produce legal or similarly
11   significant effects concerning the consumer.
12   b. A controller that has lawfully obtained personal data about a
13   consumer from a source other than the consumer shall be deemed in
14   compliance with a consumer's request to delete such data pursuant
15   to this subsection by:
16   (1) retaining a record of the deletion request and the minimum
17   data necessary for the purpose of ensuring the consumer's personal
18   data remains deleted from the controller's records and not using
19   such retained information for any other purpose pursuant to the
20   provisions of P.L.   , c.   (C.   ) (pending before the Legislature
21   as this bill); or
22   (2) deleting such personal data.**2**
23
24   **2**8. a. A consumer may designate another person to serve as the
25   consumer's authorized agent and act on the consumer's behalf to
26   opt out of the processing and sale of the consumer's personal data.
27   A consumer may designate an authorized agent using technology,
28   including a link to an Internet website, an Internet browser setting
29   or extension, or a global setting on an electronic device, that allows
30   the consumer to indicate the consumer's intent to opt-out of the
31   collection and processing for the purpose of any sale of data or for
32   the purpose of targeted advertising or **3**, when such technology
33   exists,**3** for profiling in furtherance of decisions that produce legal
34   or similarly significant effects concerning a consumer. A controller
35   shall comply with an opt-out request received from an authorized
36   agent under this subsection if the controller is able to verify, with
37   commercially reasonable effort, the identity of the consumer and
38   the authorized agent's authority to act on the consumer's behalf.
39   b. (1) Beginning not later than **3**[four] six**3** months following the
40   effective date of P.L.   , c.   (C.   ) (pending before the
41   Legislature as this bill), a controller that processes personal data for
42   purposes of targeted advertising, **3**or**3** the sale of personal data **3**[,
43   profiling in furtherance of decisions that produce legal or similarly
44   significant effects concerning a consumer]**3** shall allow consumers
45   to exercise the right to opt-out of such processing through a user-
46   selected universal opt-out mechanism.
47   (2) The platform, technology, or mechanism shall:

1   (a) not permit its manufacturer to unfairly disadvantage another
2   controller;
3   (b) not make use of a default setting that opts-in a consumer to
4   the processing or sale of personal data, unless the controller has
5   determined that the consumer has selected such default setting and
6   the selection clearly represents the consumer's **³[**an**]³** affirmative,
7   freely given, and unambiguous choice to **³[**opt-out of**]** opt into**³** any
8   processing of such consumer's personal data pursuant to P.L.   , c.
9   (C.   ) (pending before the Legislature as this bill);
10   (c) be consumer-friendly, clearly described, and easy to use by
11   the average consumer;
12   (d) be as consistent as possible with any other similar platform,
13   technology, or mechanism required by any federal or state law or
14   regulation; and
15   (e) enable the controller to accurately determine whether the
16   consumer is a resident of this State and whether the consumer has
17   made a legitimate request to opt out of the processing of personal
18   data for the purposes of any sale of such consumer's personal data
19   or targeted advertising **³[**; and
20   (3) Controllers shall inform consumers about the opt-out choices
21   available under P.L.   , c.   (C.   ) (pending before the
22   Legislature as this bill)**]³**.
23   c. The Division of Consumer Affairs in the Department of Law
24   and Public Safety may adopt rules and regulations that detail the
25   technical specifications for one or more universal opt-out
26   mechanisms that clearly communicate a consumer's affirmative,
27   freely given, and unambiguous choice to opt out of the processing
28   of personal data pursuant to P.L.   , c.   (C.   ) (pending before
29   the Legislature as this bill), including regulations that permit the
30   controller to accurately authenticate the consumer as a resident of
31   this state and determine that the mechanism represents a legitimate
32   request to opt out of the processing of personal data pursuant to
33   P.L.   , c.   (C.   ) (pending before the Legislature as this bill).
34   The division may update the rules that detail the technical
35   specifications for the mechanisms from time to time to reflect the
36   means by which consumers interact with controllers.**²**
37
38   **²**9. a. A controller shall:
39   (1) limit the collection of personal data to what is adequate,
40   relevant, and reasonably necessary in relation to the purposes for
41   which such data is processed, as disclosed to the consumer;
42   (2) except as otherwise provided in P.L.   , c.   (C.   )
43   (pending before the Legislature as this bill), not process personal
44   data for purposes that are neither reasonably necessary to, nor
45   compatible with, the purposes for which such personal data is
46   processed, as disclosed to the consumer, unless the controller
47   obtains the consumer's consent;

1   (3) take reasonable measures to establish, implement, and
2   maintain administrative, technical, and physical data security
3   practices to protect the confidentiality, integrity, and accessibility of
4   personal data and to secure personal data during both storage and
5   use from unauthorized acquisition. The data security practices shall
6   be appropriate to the volume and nature of the personal data at
7   issue;
8   (4) not process sensitive data concerning a consumer without
9   first obtaining the consumer's consent, or, in the case of the
10   processing of personal data concerning a known child, without
11   processing such data in accordance with COPPA;
12   (5) not process personal data in violation of the laws of this State
13   and federal laws that prohibit unlawful discrimination against
14   consumers;
15   (6) provide an effective mechanism for a consumer to revoke the
16   consumer's consent under this section that is at least as easy as the
17   mechanism by which the consumer provided the consumer's
18   consent and, upon revocation of such consent, cease to process the
19   data as soon as practicable, but not later than 15 days after the
20   receipt of such request;
21   (7) not process the personal data of a consumer for purposes of
22   targeted advertising, the sale of the consumer's personal data, or
23   profiling in furtherance of decisions that produce legal or similarly
24   significant effects concerning a consumer without the consumer's
25   consent, under circumstances where a controller has actual
26   knowledge, or willfully disregards, that the consumer is at least 13
27   years of age but younger than 17 years of age;
28   (8) specify the express purposes for which personal data are
29   processed; and
30   (9) not conduct processing that presents a heightened risk of
31   harm to a consumer without conducting and documenting a data
32   protection assessment of each of its processing activities that
33   involve personal data acquired on or after the effective date of
34   P.L.   , c.   (C.   ) (pending before the Legislature as this bill)
35   that present a heightened risk of harm to a consumer.
36   b. Data protection assessments shall identify and weigh the
37   benefits that may flow, directly and indirectly, from the processing
38   to the controller, the consumer, other stakeholders, and the public
39   against the potential risks to the rights of the consumer associated
40   with the processing, as mitigated by safeguards that the controller
41   can employ to reduce the risks. The controller shall factor into this
42   assessment the use of de-identified data and the reasonable
43   expectations of consumers, as well as the context of the processing
44   and the relationship between the controller and the consumer whose
45   personal data will be processed. A controller shall make the data
46   protection assessment available to the Division of Consumer Affairs
47   in the Department of Law and Public Safety upon request. The
48   division may evaluate the data protection assessment for

1 compliance with the duties contained in this section and with other
2 laws. Data protection assessments shall be confidential and exempt
3 from public inspection under P.L.1963 c.3 (C.47:1A-1 et al.). The
4 disclosure of a data protection assessment pursuant to a request
5 from the division under this section shall not constitute a waiver of
6 any attorney-client privilege or work-product protection that might
7 otherwise exist with respect to the assessment and any information
8 contained in the assessment.
9   c. For the purposes of this section, "heightened risk" includes:
10   (1) processing personal data for purposes of targeted advertising
11 or for profiling if the profiling presents a reasonably foreseeable
12 risk of: unfair or deceptive treatment of, or unlawful disparate
13 impact on, consumers; financial or physical injury to consumers; a
14 physical or other intrusion upon the solitude or seclusion, or the
15 private affairs or concerns, of consumers if the intrusion would be
16 offensive to a reasonable person; or other substantial injury to
17 consumers;
18   (2) selling personal data; and
19   (3) processing sensitive data.**²**
20   **³**d. A single data protection assessment may address a
21 comparable set of processing operations that include similar
22 activities.**³**
23
24   **²**10. Nothing in P.L.   , c.   (C.   ) (pending before the
25 Legislature as this bill) shall apply to:
26   a.   protected health information collected by a covered entity or
27 business associate subject to the privacy, security, and breach
28 notification rules issued by the United States Department of Health
29 and Human Services, Parts 160 and 164 of Title 45 of the Code of
30 Federal Regulations, established pursuant to the "Health Insurance
31 Portability and Accountability Act of 1996," Pub.L.104-191, and
32 the "Health Information Technology for Economic and Clinical
33 Health Act," 42 U.S.C. s.17921 et seq.;
34   b.   a financial institution **³**, data,**³** or an affiliate of a financial
35 institution that is subject to Title V of the federal "Gramm-Leach-
36 Bliley Act," 15 U.S.C. s.6801 et seq., and the rules and
37 implementing regulations promulgated thereunder;
38   c.   the secondary market institutions identified in
39 15 U.S.C. s.6809(3)(D) and 12 C.F.R. s.1016.3(l)(3)(iii);
40   d.   an insurance institution subject to P.L.1985, c.179
41 (C.17:23A-1 et seq.);
42   e.   the sale of a consumer's personal data by the New Jersey
43 Motor Vehicle Commission that is permitted by the federal
44 "Drivers' Privacy Protection Act of 1994," 18 U.S.C. s.2721 et seq.;
45   f. personal data collected, processed, sold, or disclosed by a
46 consumer reporting agency, as defined in 15 U.S.C. s.1681a(f), if
47 the collection, processing, sale, or disclosure of the personal data is

1   limited, governed, and collected, maintained, disclosed, sold,
2   communicated, or used only as authorized by the federal "Fair
3   Credit Reporting Act," 15 U.S.C. s.1681 et seq., and implementing
4   regulations;
5   g. any State agency as defined in section 2 of P.L.1971, c.182
6   (C.52:13D-13), any political subdivision, and any division, board,
7   bureau, office, commission, or other instrumentality created by a
8   political subdivision; or
9   h personal data that is collected, processed, or disclosed, as
10 part of research conducted in accordance with the Federal Policy for
11 the protection of human subjects pursuant to 45 C.F.R. Part 46 or
12 the protection of human subjects pursuant to 21 C.F.R. Parts 50 and
13 56.[2]

14

15   [2]11. Nothing in P.L. , c.   (C.   ) (pending before the
16 Legislature as this bill) shall require [3][an operator] a controller[3] to:
17   a.   re-identify de-identified data;
18   b.   collect, retain, use, link, or combine personal data
19 concerning a consumer that it would not otherwise collect, retain,
20 use, link, or combine in the ordinary course of business.[2]

21

22   [2]12. a. Nothing in P.L. , c.   (C.   ) (pending before the
23 Legislature as this bill) shall be construed to restrict a controller's
24 or processor's ability to:
25   (1) comply with federal or State law or regulations;
26   (2) comply with a civil, criminal or regulatory inquiry,
27 investigation, subpoena or summons by federal, State, municipal or
28 other governmental authorities;
29   (3) cooperate with law enforcement agencies concerning conduct
30 or activity that the controller or processor reasonably and in good
31 faith believes may violate federal, State or municipal ordinances or
32 regulations;
33   (4) investigate, establish, exercise, prepare for or defend legal
34 claims;
35   (5) provide a product or service specifically requested by a
36 consumer;
37   (6) perform under a contract to which a consumer is a party,
38 including fulfilling the terms of a written warranty;
39   (7) take steps at the request of a consumer prior to entering into a
40 contract;
41   (8) take immediate steps to protect an interest that is essential for
42 the life or physical safety of the consumer or another individual,
43 and where the processing cannot be manifestly based on another
44 legal basis;
45   (9) prevent, detect, protect against or respond to security
46 incidents, identity theft, fraud, harassment, malicious or deceptive
47 activities or any illegal activity, preserve the integrity or security of

1 systems or investigate, report or prosecute those responsible for any
2 such action;
3   (10) engage in public or peer-reviewed scientific or statistical
4 research in the public interest that adheres to all other applicable
5 ethics and privacy laws and is approved, monitored and governed
6 by an institutional review board that determines, or similar
7 independent oversight entities that determine,
8   (a) whether the deletion of the information is likely to provide
9 substantial benefits that do not exclusively accrue to the controller,
10   (b) the expected benefits of the research outweigh the privacy
11 risks, and
12   (c) whether the controller has implemented reasonable
13 safeguards to mitigate privacy risks associated with research,
14 including any risks associated with re-identification;
15   (11) assist another controller, processor, or third party with any
16 of the obligations under P.L.   , c.   (C.   ) (pending before the
17 Legislature as this bill); or
18   (12) personal data for reasons of public interest in the area of
19 public health, community health, or population health, but solely to
20 the extent that such processing is
21   (a) subject to suitable and specific measures to safeguard the
22 rights of the consumer whose personal data is being processed, and
23   (b) under the responsibility of a professional subject to
24 confidentiality obligations under federal, State or local law.
25   b. The obligations imposed on controllers or processors under
26 P.L.   , c.   (C.   ) (pending before the Legislature as this bill)
27 shall not restrict a controller's or processor's ability to collect, use,
28 or retain data for internal use to:
29   (1) conduct internal research to develop, improve, or repair
30 products, services, or technology;
31   (2) effectuate a product recall;
32   (3) identify and repair technical errors that impair existing or
33 intended functionality; or
34   (4) perform internal operations that are reasonably aligned with
35 the expectations of the consumer or reasonably anticipated based on
36 the consumer's existing relationship with the controller, or are
37 otherwise compatible with processing data in furtherance of the
38 provision of a product or service specifically requested by a
39 consumer or the performance of a contract to which the consumer is
40 a party. Personal data collected, used, or retained pursuant to this
41 subsection shall, where applicable, take into account the nature and
42 purpose or purposes of such collection, use or retention. Such data
43 shall be subject to reasonable administrative, technical, and physical
44 measures to protect the confidentiality, integrity, and accessibility
45 of the personal data and to reduce reasonably foreseeable risks of
46 harm to consumers relating to such collection, use, or retention of
47 personal data.

1   c. The obligations imposed on controllers or processors under
2   P.L.   , c.   (C.   ) (pending before the Legislature as this bill)
3   shall not apply where compliance by the controller or processor
4   with the provisions of law would violate an evidentiary privilege
5   under the laws of this State. Nothing in P.L.   , c.   (C.   )
6   (pending before the Legislature as this bill) shall be construed to
7   prevent a controller or processor from providing personal data
8   concerning a consumer to a person covered by an evidentiary
9   privilege under the laws of the State as part of a privileged
10   communication.
11   d. Personal data that are processed by a controller pursuant to an
12   exception provided by this section:
13   (1) shall not be processed for any purpose other than a purpose
14   expressly listed in this section; and
15   (2) shall be processed solely to the extent that the processing is
16   necessary, reasonable, and proportionate to the specific purpose or
17   purposes listed in this section.
18   e. If a controller processes personal data pursuant to an
19   exemption in this section, the controller bears the burden of
20   demonstrating that such processing qualifies for the exemption and
21   complies with the requirements in this section.
22   f. Processing personal data for the purposes expressly identified
23   in this section shall not solely make a legal entity a controller with
24   respect to such processing if such entity would not otherwise meet
25   the definition of a controller.[2]
26
27   [2]13. a. Controllers and processors shall meet their respective
28   obligations established under P.L.   , c.   (C.   ) (pending before
29   the Legislature as this bill).
30   b. Processors shall adhere to the instructions of the controller and
31   assist the controller to meet its obligations under this act. Taking
32   into account the nature of processing and the information available
33   to the processor, the processor shall assist the controller by:
34   (1) taking appropriate technical and organizational measures,
35   insofar as possible, for the fulfillment of the controller's obligation
36   to respond to consumer requests to exercise their rights under this
37   act;
38   (2) helping to meet the controller's obligations in relation to the
39   security of processing the personal data and in relation to
40   notification of a breach of the security of the system; and
41   (3) providing information to the controller necessary to enable
42   the controller to conduct and document any data protection
43   assessments required by section 9 of P.L.   , c.   (C.   )
44   (pending before the Legislature as this bill). The controller and
45   processor are each responsible for only the measures allocated to
46   them.
47   c. Notwithstanding the instructions of the controller, a
48   processor shall:

1   (1) ensure that each person processing the personal data is
2   subject to a duty of confidentiality with respect to the data; and
3   (2) engage a subcontractor pursuant to a written contract in
4   accordance with subsection e. of this section that requires the
5   subcontractor to meet the obligations of the processor with respect
6   to the personal data.
7   d.   Taking into account the context of processing, the controller
8   and the processor shall implement appropriate technical and
9   organizational measures to ensure a level of security appropriate to
10   the risk and establish a clear allocation of the responsibilities
11   between them to implement the measures.
12   e.   Processing by a processor shall be governed by a contract
13   between the controller and the processor that is binding on both
14   parties and that sets forth:
15   (1) the processing instructions to which the processor is bound,
16   including the nature and purpose of the processing;
17   (2) the type of personal data subject to the processing, and the
18   duration of the processing;
19   (3) the requirements imposed by this subsection and subsections
20   c. and d. of this section; and
21   (4) the following requirements:
22   (a) At the discretion of the controller, the processor shall delete
23   or return all personal data to the controller as requested at the end of
24   the provision of services, unless retention of the personal data is
25   required by law;
26   (b) (i) The processor shall make available to the controller all
27   information necessary to demonstrate compliance with the
28   obligations in this act; and
29   (ii) The processor shall allow for, and contribute to, reasonable
30   assessments and inspections by the controller or the controller's
31   designated assessor. Alternatively, the processor may, with the
32   controller's consent, arrange for a qualified and independent
33   assessor to conduct, at least annually and at the processor's expense,
34   an assessment of the processor's policies and technical and
35   organizational measures in support of the obligations under this act
36   using an appropriate and accepted control standard or framework
37   for the assessment as applicable. The processor shall provide a
38   report of the assessment to the controller upon request.
39   f. In no event may a contract relieve a controller or a processor
40   from the liabilities imposed on them by virtue of its role in the
41   processing relationship as defined by P.L.   , c.   (C.   )
42   (pending before the Legislature as this bill).
43   g. Determining whether a person is acting as a controller or
44   processor with respect to a specific processing of data shall be a
45   fact-based determination that depends upon the context in which
46   personal data are to be processed. A person that is not limited in its
47   processing of personal data pursuant to a controller's instructions, or
48   that fails to adhere to the instructions, shall be deemed a controller

1   and not a processor with respect to a specific processing of data. A
2   processor that continues to adhere to a controller's instructions with
3   respect to a specific processing of personal data shall remain a
4   processor. If a processor begins, alone or jointly with others,
5   determining the purposes and means of the processing of personal
6   data, it shall be deemed a controller with respect to the processing.**2**

7

8   **2**14.   a.   It shall be an unlawful practice and violation of
9   P.L.1960, c.39 (C.56:8-1 et seq.) for a controller to violate the
10 provisions of P.L.   , c.   (C.   ) (pending before the Legislature
11 as this bill).
12   b.   Until the first day of the 18th month next following the
13 effective date of P.L.   , c.   (C.   ) (pending before the
14 Legislature as this bill), prior to bringing an enforcement action
15 before an administrative law judge or a court of competent
16 jurisdiction in this State, the Division of Consumer Affairs in the
17 Department of Law and Public Safety shall issue a notice to the
18 controller if a cure is deemed possible. If the operator controller
19 fails to cure the alleged violation of P.L.   , c.   (C.   ) (pending
20 before the Legislature as this bill) within 30 days after receiving
21 notice of alleged noncompliance from the division, such
22 enforcement action may be brought.**2**

23

24   **2**[9.] 15.**2**   The Director of the Division of Consumer Affairs in
25 the Department of Law and Public Safety shall promulgate rules
26 and regulations, pursuant to the "Administrative Procedure Act,"
27 P.L.1968, c.410 (C.52:14B-1 et seq.), necessary to effectuate the
28 purposes of P.L.   , c.   (C.   ) (pending before the Legislature as
29 this bill).

30

31   **2**[10.] 16.**2**   The Office of the Attorney General shall have sole
32 and   exclusive   authority   to   enforce   a   violation   of
33 P.L.   , c. (C.   ) (pending before the Legislature as this bill).
34 **1**Nothing in P.L.   , c.   (C.   ) (pending before the Legislature
35 as this bill) shall be construed as providing the basis for, or subject
36 to, a private right of action for violations of P.L.   , c.   (C.   )
37 (pending before the Legislature as this bill) **3**[or under any other
38 law]**3**.**1**

39

40   **2**[11] 17**2**.   This act shall take effect on the **2**[180th] 365th**2** day
41 following the date of enactment, except that the Director of the
42 Division   of   Consumer   Affairs   may   take   any   anticipatory
43 administrative action in advance as shall be necessary for the
44 implementation of this act.