GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2023

SENATE BILL 525

Short Title:	Consumer Privacy Act.	(Public)
Sponsors:	Senators Salvador, Moffitt, and Hanig (Primary Sponsors).	
Referred to:	Rules and Operations of the Senate	

April 4, 2023

A BILL TO BE ENTITLED

AN ACT TO PROTECT CONSUMERS BY ENACTING THE CONSUMER PRIVACY ACT OF NORTH CAROLINA.

The General Assembly of North Carolina enacts:

SECTION 1. This act shall be known and may be cited as the "North Carolina Consumer Privacy Act."

SECTION 2. The General Statutes are amended by adding a new Chapter to read:

"**Chapter 75F.**

"**Consumer Privacy Act.**

"**§ 75F-1. Definitions.**

(a) This Chapter shall be known and may be cited as the "North Carolina Consumer Privacy Act."

(b) Definitions. – The following definitions apply in this Chapter:

(1) Account. – The Consumer Privacy Restricted Account established in G.S. 75F-14.

(2) Affiliate. – An entity that (i) controls, is controlled by, or is under common control with another entity or (ii) shares common branding with another entity.

(3) Aggregated data. – Information that relates to a group or category of consumers (i) from which individual consumer identities have been removed and (ii) that is not linked or reasonably linkable to any consumer.

(4) Air carrier. – As defined in 49 U.S.C. § 40102.

(5) Authenticate. – To use reasonable means to determine that a consumer's request to exercise the rights described in G.S. 75F-4 is made by the consumer who is entitled to exercise those rights.

(6) Biometric data. – Data generated by automatic measurements of an individual's unique biological characteristics. The term includes an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual. Biometric data does not include any of the following:

a. A physical or digital photograph.

b. A video or audio recording.

c. Data generated from an item described in sub-subdivision a. or b. of this subdivision.

d. Information captured from a patient in a health care setting.

e. Information collected, used, or stored for treatment, payment, or health care operations as those terms are defined in 45 C.F.R. Parts 160, 162, and 164.

(7) Business associate. – As defined in 45 C.F.R. § 160.103.

(8) Child. – An individual younger than 13 years old.

(9) Consent. – An affirmative act by a consumer that unambiguously indicates the consumer's voluntary and informed agreement to allow a person to process personal data related to the consumer.

(10) Consumer. – An individual who is a resident of this State acting in an individual or household context. The term does not include an individual acting in a commercial or employment context.

(11) Control or controlled. – Includes each of the following: (i) ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting securities of an entity; (ii) control in any manner over the election of a majority of the directors or of the individuals exercising similar functions; and (iii) the power to exercise controlling influence of the management of an entity.

(12) Controller. – A person doing business in this State who determines the purposes for which, and the means by which, personal data are processed, regardless of whether the person makes the determination alone or with others that, alone or jointly with others, determines the purpose and means of processing personal data.

(13) Covered entity. – As defined in 45 C.F.R. § 160.103.

(14) De-identified data. – Data that cannot reasonably be linked to an identified or identifiable individual that are possessed by a controller who does all of the following:

a. Takes reasonable measures to ensure that a person cannot associate the data with an individual.

b. Publicly commits to maintain and use the data only in de-identified form and not attempt to reidentify the data.

c. Contractually obligates any recipients of the data to comply with the requirements described in sub-subdivisions a. and b. of this subdivision.

(15) Director. – The Director of the Division.

(16) Division. – Consumer Protection Division of the North Carolina Department of Justice or other unit of the Department of Justice engaging in activities under this Chapter.

(17) Government entity. – The State or any local political subdivision of the State.

(18) Health care facility. – Any entity licensed pursuant to Chapter 122C, 131D, or 131E of the General Statutes or Article 64 of Chapter 58 of the General Statutes, and any clinical laboratory certified under the federal Clinical Laboratory Improvement Amendments in section 353 of the Public Health Service Act (42 U.S.C. § 263a).

(19) Health care provider. – Includes:

a. An individual who is licensed, certified, or otherwise authorized under Chapter 90 or 90B of the General Statutes to provide health care services in the ordinary course of business or practice of a profession or in an approved education or training program.

b. A health care facility where health care services are provided to patients, residents, or others to whom such services are provided as allowed by law.

c. Individuals licensed under Chapter 90 of the General Statutes or practicing under a waiver in accordance with G.S. 90-12.5.
d. Any emergency medical services personnel as defined in G.S. 131E-155(7).
e. Any individual who is employed as a health care facility administrator, executive, supervisor, board member, trustee, or other person in a managerial position or comparable role at a health care facility.
f. An agent or employee of a health care facility that is licensed, certified, or otherwise authorized to provide health care services.
g. An officer or director of a health care facility.
h. An agent or employee of a health care provider who is licensed, certified, or otherwise authorized to provide health care services.

(20) Identifiable individual. – An individual who can be readily identified, directly or indirectly.

(21) Institution of higher education. – A public or private institution of higher education.

(22) Local political subdivision. – Includes a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college.

(23) Nonprofit organization. – Any corporation exempt from taxation under section 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code.

(24) Personal data. – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information. The term does not include information that is a public record under Chapter 132 of the General Statutes or information made available to the general public lawfully and intentionally.

(25) Process. – Any operation or set of operations performed on personal data, including collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(26) Processor. – A person who processes personal data on behalf of a controller.

(27) Protected health information. – As defined in 45 C.F.R. § 160.103.

(28) Pseudonymous data. – Personal data that cannot be attributed to a specific individual without the use of additional information, if the additional information is (i) kept separately from the consumer's personal data and (ii) subject to appropriate technical and organizational measures to ensure that the personal data is not attributable to an identified or identifiable individual.

(29) Publicly available information. – Information that a person (i) lawfully obtains from a record of a governmental entity, (ii) reasonably believes a consumer or widely distributed media has lawfully made available to the general public, or (iii) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

(30) Right. – A consumer right described in G.S. 75F-4.

(31) Sale, sell, or sold. – The exchange of personal data for monetary consideration by the controller to a third party. The terms do not include any of the following:

a. A controller's disclosure of personal data to a processor who processes the personal data on behalf of the controller.
b. A controller's disclosure of personal data to an affiliate of the controller.
c. Considering the context in which the consumer provided the personal data to the controller, a controller's disclosure of personal data to a

third party if the purpose is consistent with a consumer's reasonable expectations.

d. The disclosure or transfer of personal data when a consumer directs a controller to disclose the personal data or interact with one or more third parties.

e. A consumer's disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of a child.

f. The disclosure of information that the consumer intentionally makes available to the general public via a channel of mass media and does not restrict to a specific audience.

g. A controller's transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, or bankruptcy in which the third party assumes control of all or part of the controller's assets.

(32) Sensitive data. – Personal data that reveals any of the following:

a. An individual's (i) racial or ethnic origin, (ii) religious beliefs, (iii) sexual orientation, (iv) citizenship or immigration status, or (v) information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional. The term does not include personal data that reveals an individual's racial or ethnic origin if the personal data are processed by a video communication service. If the personal data are processed by a person licensed to provide health care under State or federal law, information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional, then the personal data is not sensitive data.

b. The processing of genetic or biometric data if the processing is for the purpose of identifying a specific individual.

c. Specific geolocation data.

(33) Specific geological location. – Information derived from technology, including global positioning system level latitude and longitude coordinates, that directly identifies an individual's specific location, accurate within a radius of 1,750 feet or less. The term does not include (i) the content of a communication or (ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment used by a utility.

(34) Targeted advertising. – Displaying an advertisement to a consumer where the consumer is selected based upon personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences and interests. The term does not include any advertising:

a. Based upon a consumer's activities within the controller's website or online application or any affiliated website or online application.

b. Based on the context of a consumer's current search query or visit to a website or online application.

c. Directed to a consumer in response to the consumer's request for information, product, a service, or feedback.

d. Processing personal data solely to measure or report advertising performance, reach, or frequency.

(35) Third party. – A person other than the consumer, controller, or processor or an affiliate or contractor of the controller or processor.

(36) Trade secret. – Information, including a formula, pattern, compilation, program, device, method, technique, or process that (i) derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means by other persons who can obtain economic value from the information's disclosure or use and (ii) is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

"**§ 75F-2. Applicability.**

(a) This Chapter applies to any controller or processor who:

(1) Conducts business in this State or produces a product or service that is targeted to consumers who are residents of this State;

(2) Has annual revenue of twenty-five million dollars ($25,000,000) or more; and

(3) Satisfies one or more of the following thresholds:

a. During a calendar year, controls or processes personal data of 100,000 or more consumers; or

b. Derives over fifty percent (50%) of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

(b) This Chapter does not apply to any of the following:

(1) A governmental entity or a third party under contract with a governmental entity when the third party is acting on behalf of the governmental entity.

(2) A tribe.

(3) An institution of higher education.

(4) A nonprofit corporation.

(5) A covered entity.

(6) A business associate.

(7) Information that meets the definition of one of the following:

a. Protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., and related regulations.

b. Patient identifying information for purposes of 42 C.F.R. Part 2.

c. Identifiable private information for purposes of the federal Policy for the Protection of Human Subjects, 45 C.F.R. Part 46.

d. Identifiable private information or personal data collected as part of human subjects research pursuant to or under the same standards as:

1. The good clinical practice guidelines issued by the International Council for Harmonisation; or

2. The Protection of Human Subjects under 21 C.F.R. Part 50 and Institutional Review Boards under 21 C.F.R. Part 56.

e. Personal data used or shared in research conducted in accordance with one or more of the requirements described in sub-subdivision b. of this subdivision.

f. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11101 et seq., and related regulations.

g. Patient safety work product for purposes of 42 C.F.R. Part 3; or

h. Information that is:

1. De-identified in accordance with the requirements for de-identification set forth in 45 C.F.R. Part 164; and

2. Derived from any of the health care-related information listed above in this subdivision.

(8) Information originating from, and intermingled to be indistinguishable with, information under subdivision (7) of this subsection that is maintained by a (i) health care facility or health care provider or (ii) program or a qualified service organization as defined in 42 C.F.R. § 2.11.

(9) Information used only for public health activities and purposes as described in 45 C.F.R. § 164.512.

(10) An activity:

a. Subject to regulation under the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., by one of the following:

1. A consumer reporting agency, as defined in 15 U.S.C. § 1681a;

2. A furnisher of information, as set forth in 15 U.S.C. § 1681s-2, who provides information for use in a consumer report, as defined in 15 U.S.C. § 1681a; or

3. A user of a consumer report, as set forth in 15 U.S.C. § 1681b; and

b. Involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.

(11) A financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., and related regulations.

(12) Personal data collected, processed, sold, or disclosed in accordance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq.

(13) Personal data regulated by the federal Family Education Rights and Privacy Act, 20 U.S.C. § 1232g, and related regulations.

(14) Personal data collected, processed, sold, or disclosed in accordance with the federal Farm Credit Act of 1971, 12 U.S.C. § 2001 et seq.

(15) Data that are processed or maintained:

a. In the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party to the extent the collection and use of the data are related to the individual's role;

b. As the emergency contact information of an individual described in sub-subdivision a. of this subdivision and used for emergency contact purposes; or

c. To administer benefits for another individual relating to an individual described in sub-subdivision a. of this subdivision and used for the purpose of administering the benefits.

(16) An individual's processing of personal data for purely personal or household purposes.

(17) An air carrier.

(c) A controller is in compliance with any obligation to obtain parental consent under this Chapter if the controller complies with the verifiable parental consent mechanisms under the Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq., and the act's implementing regulations and exemptions.

(d) This Chapter does not require a person to take any action in conflict with the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., or related regulations.

"**§ 75F-3. Preemption; reference to other laws.**

(a) This Chapter supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a local political subdivision of the State regarding the processing of personal data by a controller or processor.

(b) Any reference to federal law in this Chapter includes any rules or regulations promulgated under the federal law.

"**§ 75F-4. Consumer rights; access; deletion; portability; opt out of certain processing.**

(a) A consumer has the right to:

(1) Confirm whether a controller is processing the consumer's personal data and access the consumer's personal data.

(2) Delete the consumer's personal data that the consumer provided to the controller.

(3) Obtain a copy of the consumer's personal data that the consumer previously provided to the controller, in a format that to the extent technically feasible, that is readily usable and allows the consumer to transmit the data to another controller without impediment where the processing is carried out by automated means.

(4) Opt out of the processing of the consumer's personal data for purposes of targeted advertising or the sale of personal data.

(b) Nothing in this section requires a person to cause a breach of security system.

"**§ 75F-5. Exercising consumer rights.**

(a) A consumer may exercise a right by submitting a request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise.

(b) In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise a right on the child's behalf.

(c) In the case of processing personal data concerning a consumer subject to guardianship, the guardian of the consumer shall exercise a right on the consumer's behalf.

"**§ 75F-6. Controller's response to requests.**

(a) Subject to the other provisions of this Chapter, a controller shall comply with a consumer's request under G.S. 75F-5 to exercise a right.

(b) Within 45 days after the day on which a controller receives a request to exercise a right, the controller shall take action on the consumer's request and inform the consumer of any action taken on the consumer's request.

(c) The controller may extend once the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller. If a controller extends the initial 45-day period, before the initial 45-day period expires, the controller shall (i) inform the consumer of the extension, including the length of the extension, and (ii) provide the reasons the extension is reasonably necessary.

(d) The 45-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent and the controller is not able to authenticate the request before the 45-day period expires.

(e) If, in accordance with this section, a controller chooses not to take action on a consumer's request, the controller shall within 45 days after the day on which the controller receives the request inform the consumer of the reasons for not taking action.

(f) A controller may not charge a fee for information in response to a request, unless the request is the consumer's second or subsequent request during the same 12-month period. However, a controller may charge a reasonable fee to cover the administrative costs of complying with a request or refuse to act on a request if:

(1) The request is excessive, repetitive, technically infeasible, or manifestly unfounded;

(2) The controller reasonably believes the primary purpose in submitting the request was something other than exercising a right; or

(3) The request, individually or as part of an organized effort, harasses, disrupts, or imposes undue burden on the resources of the controller's business.

(g) A controller that charges a fee or refuses to act in accordance with this section bears the burden of demonstrating the request satisfied one or more of the criteria described in this section.

(h) If a controller is unable to authenticate a consumer request to exercise a right described in G.S. 75F-4 using commercially reasonable efforts, the controller is not required to comply with the request and may request that the consumer provide additional information reasonably necessary to authenticate the request.

"**§ 75F-7. Responsibilities according to role.**

(a) A processor shall adhere to the controller's instructions, and taking into account the nature of the processing and information available to the processor, by appropriate technical and organizational measures, insofar as reasonably practicable, assist the controller in meeting the controller's obligations, including obligations related to the security of processing personal data and notification of a breach of security system.

(b) Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that does all of the following:

(1) Clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations.

(2) Requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data.

(3) Requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

(c) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor.

"**§ 75F-8. Responsibilities of contractors; transparency; purpose specification and data minimization; consent for secondary use; security; nondiscrimination.**

(a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes all of the following:

(1) The categories of personal data processed by the controller.

(2) The purposes for which the categories of personal data are processed.

(3) How consumers may exercise a right.

(4) The categories of personal data that the controller shares with third parties, if any.

(5) The categories of third parties, if any, with whom the controller shares personal data.

If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the sale of the consumer's personal data or processing for targeted advertising.

(b) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to protect the confidentiality and integrity of personal data and reduce reasonably foreseeable risks of harm to consumers relating to the

processing of personal data. Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

(c) Except as otherwise provided in this Chapter, a controller may not process sensitive data collected from a consumer without first presenting the consumer with clear notice and an opportunity to opt out of the processing, or in the case of the processing of personal data concerning a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq., and the act's implementing regulations and exemptions.

(d) A controller may not discriminate against a consumer for exercising a right by (i) denying a good or service to the consumer, (ii) charging the consumer a different price or rate for a good or service, or (iii) providing the consumer a different level of quality of a good or service. Nothing in this subsection prohibits a controller from offering a different price, rate, level, quality, or selection of a good or service to a consumer, including offering a good or service for no fee or at a discount, if the consumer has opted out of targeted advertising or the offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(e) A controller is not required to provide a product, service, or functionality to a consumer if the consumer's personal data are, or the processing of the consumer's personal data is, reasonably necessary for the controller to provide the consumer the product, service, or functionality and the consumer does not provide the consumer's personal data to the controller or allow the controller to process the consumer's personal data. Any provision of a contract that purports to waive or limit a consumer's right under this Chapter is void.

"**§ 75F-9. Processing de-identified data or pseudonymous data.**

(a) The provisions of this Chapter do not require a controller or processor to do any of the following:

(1) Reidentify de-identified data or pseudonymous data.

(2) Maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data.

(3) Comply with an authenticated consumer request to exercise a right described in G.S. 75F-4, if the controller:

a. Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

b. Does not (i) use the personal data to recognize or respond to the consumer who is the subject of the personal data or (ii) associate the personal data with other personal data about the consumer; and

c. Does not sell or other otherwise disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(b) The rights described in G.S. 75F-4(a)(1) through (a)(3) do not apply to pseudonymous data if a controller demonstrates that any information necessary to identify a consumer is kept separately and subject to appropriate technical and organizational measures to ensure the personal data are not attributed to an identified individual or an identifiable individual.

(c) A controller who uses pseudonymous data or de-identified data shall take reasonable steps to ensure the controller complies with any contractual obligations to which the pseudonymous data or de-identified data are subject and promptly addresses any breach of a contractual obligation.

"**§ 75F-10. Limitations.**

(a) The requirements described in this Chapter do not restrict a controller's or processor's ability to do any of the following:

(1) Comply with a State, federal, or local law, rule, or regulation.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, State, local, or other governmental entity.

(3) Cooperate with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, State, or local laws, rules, or regulations.

(4) Investigate, establish, exercise, prepare for, or defend a legal claim.

(5) Provide a product or service requested by a consumer or a parent or legal guardian of a child.

(6) Perform a contract to which the consumer or the parent or legal guardian of a child is a party, including fulfilling the terms of a written warranty or taking steps at the request of the consumer or parent or legal guardian before entering into the contract with the consumer.

(7) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual.

(8) Detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity or investigate, report, or prosecute a person responsible for an action described in this subdivision.

(9) Preserve the integrity or security of systems or investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems.

(10) If the controller discloses the processing in a notice described in G.S. 75F-8, engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws.

(11) Assist another person with an obligation described in this subsection.

(12) Process personal data to do any of the following:

a. Conduct internal analytics or other research to develop, improve, or repair a controller's or processor's product, service, or technology.

b. Identify and repair technical errors that impair existing or intended functionality.

c. Effectuate a product recall.

(13) Process personal data to perform an internal operation that is (i) reasonably aligned with the consumer's expectations based on the consumer's existing relationship with the controller or (ii) otherwise compatible with processing to aid the controller or processor in providing a product or service specifically requested by a consumer or a parent or legal guardian of a child or the performance of a contract to which the consumer or a parent or legal guardian of a child is a party.

(14) Retain a consumer's email address to comply with the consumer's request to exercise a right.

(b) This Chapter does not apply if a controller's or processor's compliance with this Chapter:

(1) Violates an evidentiary privilege under North Carolina law.

(2) As part of a privileged communication, prevents a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under North Carolina law.

(3) Adversely affects the privacy or other rights of any person.

(c) A controller or processor is not in violation of this Chapter if:
(1) The controller or processor discloses personal data to a third-party controller or processor in compliance with this Chapter.
(2) The third party processes the personal data in violation of this Chapter.
(3) The disclosing controller or processor did not have actual knowledge of the third party's intent to commit a violation of this Chapter.

(d) If a controller processes personal data under an exemption described in subsection (a) of this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption.

(e) Nothing in this Chapter requires a controller, processor, third party, or consumer to disclose a trade secret.

"**§ 75F-11. No private cause of action.**

A violation of this Chapter does not provide a basis for, nor is a violation of this Chapter subject to, a private right of action under this Chapter or any other law.

"**§ 75F-12. Enforcement.**

(a) The Division shall establish and administer a system to receive consumer complaints regarding a controller's or processor's alleged violation of this Chapter.

(b) The Division may investigate a consumer complaint to determine whether the controller or processor violated or is violating this Chapter.

"**§ 75F-13. Enforcement powers of the Attorney General.**

(a) The Attorney General has the exclusive authority to enforce this Chapter. Upon referral from the Division, the Attorney General may initiate an enforcement action against a controller or processor for a violation of this Chapter.

(b) At least 45 days before the day on which the Attorney General initiates an enforcement action against a controller or processor, the Attorney General shall provide the controller or processor with the following:
(1) Written notice identifying each provision of this Chapter the Attorney General alleges the controller or processor has violated or is violating.
(2) An explanation of the basis for each allegation.

(c) The Attorney General may not initiate an action if the controller or processor:
(1) Cures the noticed violation within 45 days after the day on which the controller or processor receives the written notice described in subsection (b) of this section.
(2) Provides the Attorney General an express written statement that the violation has been cured and no further violation of the cured violation will occur.

(d) The Attorney General may initiate an action against a controller or processor who (i) fails to cure a violation after receiving the notice described in subsection (b) of this section or (ii) after curing a noticed violation and providing a written statement in accordance with subsection (b) of this section, continues to violate this Chapter.

(e) In an action described in subsection (d) of this section, the Attorney General may recover actual damages to the consumer; and for each violation described in subsection (d) of this section, an amount not to exceed seven thousand five hundred dollars ($7,500).

(f) All money received from an action under this Chapter shall be deposited into the Consumer Privacy Account established in G.S. 75F-14.

(g) If more than one controller or processor are involved in the same processing in violation of this Chapter, the liability for the violation shall be allocated among the controllers or processors in proportion to the comparative fault of each controller or processor.

"**§ 75F-14. Consumer Privacy Account.**

(a) There is created a restricted account known as the "Consumer Privacy Account." The account shall be funded by money received through civil enforcement actions under this Chapter.

(b) Upon appropriation by the General Assembly, the account funds may be used by the Attorney General for these purposes:

(1) Investigation and administrative costs incurred by the Division in investigating consumer complaints alleging violations of this Chapter.

(2) Recovery of costs and attorney fees accrued by the Attorney General in enforcing this Chapter.

(3) Providing consumer and business education regarding consumer rights under this Chapter and compliance with the provisions of this Chapter for controllers and processors.

(c) If the balance in the account exceeds four million dollars ($4,000,000) at the close of any fiscal year, the State Budget Director shall transfer the amount that exceeds four million dollars ($4,000,000) into the General Fund.

"**§ 75F-15. Attorney General report.**

(a) The Attorney General and the Division shall compile a report evaluating the liability and enforcement provisions of this Chapter, including the effectiveness of the Attorney General's and the Division's efforts to enforce this Chapter and summarizing the data protected and not protected by this Chapter, including, with reasonable detail, a list of the types of information that are publicly available from State, local, and federal government sources.

(b) The Attorney General and the Division may update the report as new information becomes available.

(c) The Attorney General and the Division shall submit the report to the Joint Legislative Oversight Commission on Governmental Operations by July 1, 2025."

SECTION 3. This act becomes effective January 1, 2024.