RETAIL ASSOCIATION OF MAINE
Voice of Maine Retail
45 Melville Street, Suite 1
Augusta, ME 04330
Phone: 207.623.1149
www.retailmaine.org

May 5, 2025

Senator Anne Carney, Chair
Representative Amy Kuhn, Chair
Members of the Judiciary Committee

RE: Testimony Regarding:

- **LD 1822 An Act to Enact the Maine Online Data Privacy Act**
- **LD 1224 An Act to Comprehensively Protect Consumer Privacy**
- **LD 1088 An Act to Enact the Maine Consumer Data Privacy Act**
- **LD 1284, An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information**

Dear Senator Carney, Representative Kuhn and members of the Judiciary Committee:

My name is Curtis Picard, and I serve as the President and CEO of the Retail Association of Maine. Our association represents retailers of all sizes from small, independent retailers, to a number of well-known Maine retail brands, and including a number of larger, multi-state retailers. Maine's retailers employ more than 80,000 Mainers, and our industry is one of the largest private sector employers in Maine.

Thank you for the opportunity to provide testimony regarding these comprehensive privacy proposals before you. We appreciate the Committee's attention to this important and complex issue, and we commend Representative Kuhn, Representative Roberts, Representative Henderson, and Senator Stewart for their commitment to protecting Maine consumers.

For the record, we are not taking a position on LD 1284. That is a narrowly focused bill related to the existing Maine ISP law.

Instead, we are focusing our testimony on LD 1224, LD 1088, and LD 1822. As veteran members of this committee know, the Retail Association of Maine, and our members, were actively involved during last year's discussion of comprehensive data privacy. I will say again what I said then – we support Maine passing comprehensive data privacy legislation. We are hopeful that this year we can reach consensus on legislation that does not put Maine businesses at a competitive disadvantage nor require a different level of compliance than other states. We are willing to work with the committee to hopefully find a path forward this year.

Moreover, this approach paradoxically removes consumer control. Instead of asking for the consumer's consent to collect sensitive data (as in LD 1224), the "strictly necessary" standard makes the judgment for them. It limits businesses from providing services that consumers may very much want—such as follow-up promotions or tailored product recommendations—even when the consumer is open to it.

Finally, enforcement under this standard becomes speculative. Regulators would be required to assess whether a business's judgment about what is "strictly necessary" is valid—a subjective and unprecise task—rather than simply reviewing a privacy notice for compliance, as they would under LD 1224.

Additionally, in the definition of Sensitive Data (Section 9602[34]): The inclusion of "billing, financial or payment method information" is vague and could be misinterpreted to include innocuous data such as purchase price or sales trends—key components of business analytics. We recommend Maine adopt the clearer definitions used in New Jersey and California. These definitions focus on financial information that, if disclosed, could grant access to a consumer's financial accounts, thereby safeguarding sensitive data without impeding standard business analytics practices.

Section 9608(2)(A): Limiting the Collection of Personal Data
This provision states that a business may only collect personal data if it is "reasonably necessary and proportionate" to provide or maintain a specific product or service requested by the consumer. As stated above, this is also language from the Maryland law which is not yet effective and therefore not yet tested.

This narrow requirement effectively bans personalized and targeted advertising, which is a vital tool for small businesses, nonprofits, and even political campaigns. These organizations rely on personalized outreach to find and serve the right audiences—without it, marketing efficiency drops and costs rise.

We appreciate that LD 1822 allows businesses to continue offering loyalty, rewards, and discount programs — a key benefit for Maine consumers, especially in the grocery and retail sectors. Consumers love loyalty and rewards programs. The average consumer in enrolled in nearly 17 different loyalty programs, and actively engages with 9 of them.

However, we are concerned that the current provision in Section 9608, Subsection 3(B), which prohibits the "sale of personal data as a condition of participation" in a loyalty program, may unintentionally restrict standard industry practices that are pro-consumer and privacy-protective.

Specifically, grocery stores and other retailers often partner with manufacturers or service providers to administer rewards. In many cases, limited customer data is shared with a supplier or processor **solely to fulfill the benefits of the loyalty program** — for example, applying a

collection, processing, and sale of data related to such individuals. While we strongly support efforts to protect younger users online—particularly young children—we are concerned that these provisions may unintentionally impair legitimate and responsible marketing practices directed at older teenagers, including those who are already participants in the economy as both consumers and workers.

Teenagers aged 15 to 17 are not only an important consumer demographic—they are also a meaningful part of the retail workforce. These young individuals make independent purchasing decisions, often with their own income, and engage with brands in the same way adults do. Applying restrictions to this entire group as if they are incapable of consumer autonomy overlooks their real-world behavior and may limit their access to relevant information about products, job opportunities, and services specifically intended for their age group. Retailers could find it legally risky or operationally unclear whether they can advertise back-to-school promotions, athletic gear, or teen-oriented brands to an audience that clearly wants and expects to receive them.

Furthermore, LD 1822 includes a provision that prohibits certain data practices when a controller *"knew or should have known"* that the consumer is a minor. This "should have known" standard is troubling. It imposes an ambiguous and highly subjective duty on businesses to assess a consumer's age, even when no age or birthdate has been collected. In many cases, especially in contexts where no account is created, it is neither practical nor possible to know—or infer—with certainty that a user is under 18. This could force businesses to take overly conservative approaches or to avoid certain kinds of content and interactions altogether, ultimately limiting access to lawful, age-appropriate services for older teens.

We recommend narrowing the application of these provisions to known children under 13, consistent with federal COPPA standards and other state frameworks, or at the very least clarifying that heightened obligations only apply when a business affirmatively knows the consumer is a minor. This would better balance the privacy rights of youth with their evolving roles as independent consumers and workers.

We also wish to express our general support for LD 1088, the Maine Consumer Data Privacy Act. This bill aligns closely with LD 1224 in its core structure and consumer protections, offering a familiar and workable framework for businesses. Notably, LD 1088 includes additional provisions that enhance consumer privacy, such as prohibiting geofencing near healthcare facilities and requiring data protection assessments for high-risk processing activities. These measures demonstrate a thoughtful approach to emerging privacy concerns and reinforce Maine's commitment to safeguarding personal data.

We appreciate the introduction of LD 1088 as part of the broader dialogue on data privacy. Its provisions contribute valuable perspectives to the conversation, and we encourage consideration of its elements in shaping comprehensive and balanced privacy legislation for Maine.

New Hampshire Data Privacy Act

On January 1, 2025, the New Hampshire Data Privacy Act ("NHDPA"), RSA 507-H, came into effect. This statute is the result of two bills, SB 255-FN and HB 1220-FN. Former Governor Chris Sununu signed SB 255-FN into law on March 6, 2024, and HB 1220-FN into law on July 19, 2024.

The following contains a summary of rights for New Hampshire consumers and a list of frequently asked questions for businesses. The information contained herein is not legal advice or an opinion from the Attorney General and should not be considered comprehensive. If consumers or businesses have questions regarding the requirements of RSA 507-H, they are encouraged to review the statute or speak with a private attorney.

If you would like to report a violation of the NHDPA, please fill out a Consumer Protection complaint form at this link or email CPB-DOJ@doj.nh.gov.

A business must provide a mechanism for you to revoke consent "that is at least as easy" as the mechanism by which you provided consent. Once the business receives your request to revoke consent, it must stop processing your data within 15 days.

How can New Hampshire consumers exercise their data privacy rights?

- You may exercise your rights by any secure and reliable means described to you in the business' privacy notice. This notice must be clear, meaningful, and reasonably accessible.

- Businesses that control data must "clearly and conspicuously" disclose how to opt out of data sales and targeted advertising. Such businesses must also provide a "clear and conspicuous" link on their website to a webpage that enables you or your agent to opt out of targeted advertising and sales of your personal data.

- You may designate an agent to exercise your opt-out rights for you. You may also opt out of targeted advertising and data sales through an opt-out preference signal or global device setting.

- A parent or legal guardian may exercise consumer rights on their child's behalf. For consumers subject to a guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise rights on the consumer's behalf.

The attorney general has exclusive authority to enforce NHDPA violations. **If you believe the NHDPA has been violated, please submit a complaint to the New Hampshire Attorney General.** Fill out a Consumer Protection complaint form at this link or email CPB-DOJ@doj.nh.gov.

What are some issues that New Hampshire consumers might encounter while trying to exercise their rights?

- Certain businesses and types of information are exempted from the NHDPA (See Below FAQs for a list of exempt businesses).

- A business which controls data can deny your rights request if it is unable to authenticate a rights request. If this happens, the business must provide you notice that it is unable to authenticate the request until you provide additional information reasonably necessary to authenticate the request. A business cannot require you to create a new account to exercise your rights.

- A business which controls data may deny an opt-out request if it has a good faith, reasonable and documented belief that your request is fraudulent. If this occurs after you try to exercise your opt-out rights, the business must send you a notice explaining that it

Frequently Asked Questions for Businesses

When did the NHDPA take effect?

RSA 507-H took effect on **January 1, 2025.**

What does the NHDPA do?

The NHDPA gives New Hampshire residents certain rights over their personal data and establishes responsibilities and privacy protection standards for entities which handle personal data (data controllers and processors).

What is "Personal Data?"

"Personal Data" is any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information. RSA 507-H:1, XIX.

What rights can New Hampshire residents exercise under the NHDPA?

New Hampshire consumers have the following rights:

- **Confirm** whether or not a controller is **processing** the consumer's personal data;
- **Access** the consumer's personal data;
- **Correct inaccuracies** in the consumer's personal data;
- **Delete** personal data provided by, or obtained about, the consumer;
- **Obtain a copy** of the consumer's personal data processed by the controller; and
- **Opt-out of the processing of the personal data for** purposes of **targeted advertising,** the **sale** of personal data, except as provided in RSA 507-H:6, **or profiling** in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

RSA 507-H:4, I.

- Mental or physical health condition or diagnosis;
- Sex life or sexual orientation;
- Citizenship or immigration status;
- The processing of genetic or biometric data for the purpose of uniquely identifying an individual;
- Personal data collected from a known child; or
- Precise geolocation data.

RSA 507-H:1, XXVIII.

What are the NHDPA requirements for processing "Sensitive Data"?

"Sensitive Data" is subject to additional restrictions under RSA 507-H. For example,

- Controllers may not process sensitive data concerning a consumer without obtaining the consumer's consent,
- Controllers may not process sensitive data concerning a known child without processing such data in accordance with COPPA, and
- Controllers must conduct and document a data protection assessment for each of the controller's processing activities that include processing sensitive data.

RSA 507-H:6, I (d), RSA 507-H:8, I.

Who is exempt from complying with the NHDPA?

The following entities are exempt from the NHDPA:

- Any State of New Hampshire body, authority, board, bureau, commission, district or agency or any political subdivision thereof;
- Any nonprofit organization;
- Any institution of higher education;
- Any national securities association that is registered under 15 U.S.C. section 78o-3 of the Securities Exchange Act of 1934;

- The protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research, as defined in 45 C.F.R. 164.501, that is conducted in accordance with the standards set forth in this chapter, or other research conducted in accordance with applicable law; RSA 507-H:3, II (e);

Certain Information and Data Regarding Professional Review Activities

- Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq.; RSA 507-H:3, II (f);

- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 U.S.C. 299b-21 et seq., as amended; RSA 507-H:3, II (g);

Certain Information about Applicants, Employees, Agents, or Independent Contractors

- Data processed or maintained in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role; as the emergency contact information of an individual under this chapter used for emergency contact purposes; or, that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under HIPPA and used for the purposes of administering such benefits; RSA 507-H:3, II (o);

Certain Information and Data Subject to Other Federal Laws

- The collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.; RSA 507-H:3, II (k);

- Personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as amended; RSA 507-H:3, II (l);

- Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g et seq., as amended; RSA 507-H:3, II (m);

- Personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 U.S.C. 2001 et seq., as amended; RSA 507-H:3, II (n);

- Personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq., as amended, by an air carrier subject to the act, to the extent this chapter is preempted by the Airline Deregulation Act, 49 U.S.C. 41713, as amended; RSA 507-H:3, II (p);

Can a consumer opt-out of the sale of personal data to third parties?

Yes, a consumer can opt-out of the sale of personal data to third parties. The controller must provide a process for submitting an opt-out request. A consumer can also designate a third party to opt-out on his or her behalf and can use an opt-out preference signal.

Can a controller deny a consumer rights request?

Yes, under certain circumstances.

If a controller is unable to authenticate a request to exercise any of the rights afforded under RSA 507-H:4, I(a)-(d) using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate the requested action. The controller must provide notice to the consumer that the controller is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the request. RSA 507-H:4, III (d).

A controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes it is fraudulent, the controller must send a notice to the person who made the request explaining that the controller believes the request is fraudulent, why the controller believes it is fraudulent and that the controller will not comply with a fraudulent request. RSA 507-H:4, III (d).

If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision. RSA 507-H:4, III (b).

Does a consumer have a right to appeal a denial?

Yes.

A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests. A controller has 60 days after receiving the appeal to inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

RSA 507-H:4, IV.

- The date the privacy notice was last updated. RSA 507-H:6, III (g).

Controllers must also clearly and conspicuously disclose the following:

- All personal data sales and targeted advertising. RSA 507-H:6, IV.
- How a consumer may opt out of data sales and targeted advertising. RSA 507-H:6, IV.
- A link on the controller's website to a targeted advertising and data sales opt-out webpage. RSA 507-H:6, V (a)(1)(A).

When must a controller seek consent before processing data?

- A controller must only process a consumer's data outside of the controller's disclosed purposes of collection if the consumer consents. RSA 507-H:6, I (b).
- A controller must only process sensitive data of a consumer if the consumer consents. RSA 507-H:6, I (d).
- A controller must allow consumer to revoke consent easily and stop processing within 15 days of consumer's revocation. RSA 507-H:6, I (f).

When must a controller conduct a data protection assessment?

If a controller processes data or causes data to be processed after July 1, 2024, that controller must conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer.

Processing that presents a heightened risk of harm to a consumer includes:

- The processing of personal data for the purposes of **targeted advertising**, RSA 507-H:8, I (a);
- The **sale** of personal data, RSA 507-H:8, I (b);
- The processing of personal data for the purposes of certain types of **profiling**, RSA 507-H:8, I (c); and
- The processing of **sensitive data**. RSA 507-H:8, I (d).

- Instructions for processing data,
- The nature and purpose of processing,
- The type of data subject to processing,
- The duration of processing, and
- The rights and obligations of both parties. RSA 507-H:7, II.

The controller-processor contract must also require that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data, RSA 507-H:7, II(a);
- At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law, RSA 507-H:7, II(b);
- Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter, RSA 507-H:7, II(c);
- After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data, RSA 507-H:7, II(d); and
- Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this law, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request. RSA 507-H:7, II(e).

Who can enforce the NHDPA?

The attorney general has exclusive authority to enforce NHDPA violations. RSA 507-H:11, I. The NHDPA does not provide for a private right of action. RSA 507-H:11, IV.

Is there a cure period?

Between January 1, 2025 and December 31, 2025

Prior to initiating an action for a violation of RSA 507-H, if the attorney general determines that a cure is possible, the attorney general will issue a notice of violation to a controller. If the