American Council of Life Insurers
American Property Casualty Insurance Association
Independent Insurance Agents of Wisconsin
National Association of Insurance and Financial Advisors - Wisconsin
National Association of Mutual Insurance Companies
Professional Insurance Agents of Wisconsin
Wisconsin Bankers Association
Wisconsin Council of Life Insurers
Wisconsin Credit Union League
Wisconsin Insurance Alliance

June 12, 2020

Data Privacy and Security Advisory Committee
Wisconsin Department of Agriculture, Trade, & Consumer Protection
2811 Agriculture Drive
P.O. Box 8911
Madison, WI 53708-8911

Dear Committee Members:

We greatly appreciate the opportunity to comment on the work of the Data Privacy and Security Advisory Committee ("DPSAC") established by the Department of Agriculture, Trade and Consumer Protection. As trade associations representing the insurance and financial services industries, our members have decades of experience operating in highly regulated environments and maintaining consumer data in a secure and confidential manner.

It is our desire and intent to continue working with state policymakers to improve data privacy and security laws. There is no doubt that the evolution of technology has given rise to legitimate privacy concerns for individuals, and state policymakers should address this issue by clearly defining expectations for consumer privacy and requiring adequate security measures to protect private and personal information.

That being said, data privacy and security laws are complex, and any regulatory scheme must weigh the preferences of consumers against the needs of businesses that process personal data. New regulations in this ever-evolving area must be developed and implemented in a manner that does not stifle innovation or frustrate consumers. Additional regulation of data privacy and security must not unnecessarily add to the already large regulatory burden imposed on Wisconsin businesses. Any significant additional regulations risk making the state less attractive for investment and growth.

Our concern is that at this point the committee may be heading toward recommendations that—while certainly well intended—may negatively impact businesses and consumers. We ask that you consider delaying recommendations for highly regulated industries or deferring to industry-specific regulators where appropriate. If action is necessary, ensure it is targeted and consistent with the existing framework.

We submit this letter to identify three important principles for future data privacy and security measures recommended by the DPSAC and other state policymakers, all with the goal of reducing harms to both businesses and consumers:

(1) **Ensure harmonization** between existing regulatory structures and requirements;

(2) **Retain and expand risk-based regulations**, which balance consumer expectations with the ability of businesses to effectively operate and innovate; and

(3) **Proceed incrementally** so that Wisconsin businesses and consumers have time to adapt and do not suddenly find themselves at a significant disadvantage.

If the DPSAC and other state policymakers respect those three important principles, they can ensure Wisconsin develops a coherent and workable data privacy and security scheme that is both business- and consumer-friendly. To provide context, we begin by describing the current state of the law, as applicable to our members, then offer our suggestions on how to best achieve these principles going forward.

I. Background: The insurance and financial services sectors are already subject to significant data privacy and security regulations.

The financial services sector already complies with many different laws regarding data breach notification, privacy, and security. Specifically, insurers and other financial institutions have been subject to comprehensive federal and state laws and regulations for many years, with additional laws currently under consideration. Prudential regulatory agencies with jurisdiction over these sectors regularly examine insurers and financial services providers to determine their compliance with these laws and regulations and test how they manage information security risk. The already-existing regulatory structure has two important effects, both of which emphasize the need for the DSPAC and other state policymakers to ensure that any new laws or regulations complement what is already in place.

First, the existing structure ensures that businesses—including our members—are already subject to a high baseline for data privacy and protection. That baseline strikes an important and delicate balance between privacy concerns and the proper use of personal information for the benefit of consumers. It is also tailored to specific industries, based on an understanding of the types of data collected and maintained by businesses, as well as the legitimate and illegitimate uses for that data.

Second, given the existing structure, any *additional* laws and regulations may cause significant confusion if not implemented carefully. As it exists now, the structure is complex. Adding more complexity amplifies the possibility that laws will conflict, either substantively (if, for instance, two laws impose different obligations) or across jurisdictions (if, for instance, Wisconsin adopts a law that is different from federal or another state's law, or subjects companies to regulation by multiple agencies within the same state).

We hope that this perspective will provide additional context for the committee regarding how certain information and industries are already regulated, so that it can understand that additional regulation may not be necessary or should respect the existing boundaries. However, in the event that the committee ultimately decides to recommend new data security and privacy measures, this information should also be valuable to ensure that new measures do not conflict with what is already in place and, instead, are consistent with other successful and similar measures across new types of information and industries.

There are three already-existing federal laws, which—when combined with related state-level regulations—impose significant data privacy and security obligations on financial services companies:

- **Fair Credit Reporting Act ("FCRA") –** FCRA imposes strict limitations on the use and sharing of intimate details of consumers' creditworthiness, reputation, and customer relationships with other companies. In general, no one is permitted to access, and reporting agencies are not permitted to disclose, such information without specific "permissible purposes." Over decades since FCRA's enactment, the Federal Trade Commission has issued guidance to enforce these limitations, such as by generally prohibiting the disclosure and use of consumer reports for marketing purposes. The Consumer Financial Protection Bureau (CFPB) now shares FCRA jurisdiction with the FTC, and it is responsible for FCRA implementing regulations, Reg. V. Fifteen (15) years ago, FCRA was amended by the Fair and Accurate Credit Transactions Act (the "FACT Act") to ensure that regulated entities implement "red flags" programs to protect against, detect, and mitigate the effects of identity theft. In addition, FCRA affords rights to consumers who have been adversely affected by information in their consumer reports. Insurers, depository institutions, non-bank lenders, and other financial services companies often use credit reports in making underwriting decisions. Accordingly, these companies are keenly aware of the limits on how consumer information may be used and are required to provide adverse action notices to individuals when a denial, cancellation, increase in charge, or adverse or unfavorable change in terms in the underwriting results from a consumer report.

- **Health Insurance Portability and Accountability Act of 1996 ("HIPAA")/ Health Information Technology for Economic and Clinical Health ("HITECH") Act –** HIPAA and HITECH protect health information maintained by covered entities, including certain insurers, along with their business associates. Among other things, it: (1) limits disclosure except in prescribed situations or with an individual's consent; (2) includes rights for individuals to request access to, amendment of, accounting of, disclosure of, and restriction on the use or disclosure of protected health information; and requires data breach notification for unauthorized disclosure of protected health information ("PHI"). Insurers are also subject to similar requirements under Wis. Admin. Code INS Chapter 25.

- **Gramm-Leach-Bliley Act ("GLBA") –** GLBA imposes privacy and security standards on financial institutions. The act broadly includes any institution which is engaged in activities that are financial in nature or incidental to such financial activities and specifically directs state insurance commissioners to adopt data privacy and data security regulations. This federal action led to the development of NAIC Model #672, which was addressed by Wisconsin in Wis. Admin. Code INS Chapter 25. The CFPB's Regulation P, which implements GLBA at the federal level, and the Office of the Insurance Commissioner's regulations in Chapter 25 require financial institutions and insurers to: (1) provide notice to consumers about privacy policies and practices; (2) describe the conditions under which nonpublic personal health information and nonpublic personal financial information about individuals may be disclosed to affiliates and nonaffiliated third parties; and (3) give individuals the opportunity to prevent a financial institution from disclosing that information to nonaffiliated third parties, specifically mandating an "opt out" option for financial information (thus allowing an individual to elect not to have their financial information shared). In addition, Chapter 25 provides consumers an "opt in" option for disclosure of health information (thus prohibiting disclosure of the individual's health information without express consent). Over the years, federal banking regulators have issued extensive guidance in response to GLBA, including requiring financial institutions to implement robust information security procedures.

- **Right of Financial Privacy Act ("RFPA") -** The RFPA establishes specific procedures that federal government authorities must follow in order to obtain information from a financial institution about a customer's financial records. Customers affected by the RFPA include individuals and partnerships of five or fewer individuals. Unless the customer has specifically consented to the release of information, such information generally can only be provided to federal law enforcement pursuant to an administrative subpoena or summons, a judicial subpoena, a search warrant, or a formal written request. A customer's consent cannot be required by the financial institution as a condition to receiving products or services. Financial institutions generally may not release financial information relating to a customer unless the government agency requesting information has provided a written certification of compliance with the RFPA. Financial institutions also must keep records of all instances in which the customer's information is disclosed to a federal government authority, including the identity of the governmental authority and a copy of the request.

II. Principle 1: Ensure harmony in the law, by focusing new recommendations on gap-filling, while also avoiding duplicative or contradictory requirements.

As the committee considers recommendations to data privacy and security laws in Wisconsin, it should harmonize those efforts with the existing framework to the maximum extent possible. The current framework provides a valuable starting point, offering the committee two benefits.

First, harmonizing any recommendations with the existing framework spares the committee from having to "reinvent the wheel." Consumers and companies already understand the existing framework. Indeed, they have years of experience and clear expectations for the treatment of sensitive data. In practice, the existing structure creates "concentric circles" of regulation—providing greater protection and control over the most sensitive information, with those protections and controls scaling down as the level of sensitivity is reduced or where the consumer has consented to use.

This model has become the accepted—and expected—approach for protecting data. Thus, future efforts to expand data privacy regulations for the financial services sector should build upon this existing structure, so that both consumers and businesses know what to expect; to the extent that any new law is necessary, it should only fill existing and identifiable gaps in that structure. Similarly, if there are new industries or specific trade practices that are of particular concern to policymakers, narrowly tailored regulations addressing those gaps should be developed. To the extent existing frameworks already exist, new regulations should be crafted within those existing structures.

Second, consideration and use of the existing framework will avoid unintended downstream confusion. There is no doubt that data-privacy regulation has important benefits to consumers and society as a whole—but *over*-regulation will be a net negative. Specifically, we want to ensure that state policymakers avoid: (1) creating duplicative requirements enforced by multiple state agencies; and (2) contradicting currently existing requirements. Complying with inconsistent laws and/or reporting to more than one state agency is a concerning possibility for business, as it risks uncertainty in expectations and enforcement while also increasing compliance costs.

In short, recommendations the committee ultimately makes should be consistent with what already exists, vesting clear authority for oversight and enforcement in the single regulatory agency for that industry as possible.

In light of the already-existing regulations, together with our hope that any additional regulations will be targeted to fill gaps and consistent with what is already in place, we specifically make the following requests of the committee:

- **Consider delaying recommendations for highly regulated industries or deferring to industry-specific regulators where appropriate.** There are several bases on which the committee may choose this path.

  - *The already-existing framework imposes significant data-protection responsibilities on businesses, including insurers.* Financial institutions already comply with the FCRA, GLBA, and RFPA, along with implementing regulations and regulatory guidance. For insurers, the Wisconsin Privacy of Consumer Financial and Health Information Regulation, adopted in response to GLBA and HIPAA, requires insurers to disclose privacy policies and practices and allows consumers to prevent disclosure of their information.

  - *Financial institutions and insurers are subject to other laws that limit their use of data.* Aside from the general protection of data, other laws also control the *use* of personal data by a financial institution or insurer. Examples include unfair discrimination and other underwriting or rating statutes regulating insurance companies, and equal credit and anti-discrimination statutes relating to the extension of credit by financial institutions. In this sense, financial institutions and insurers are prohibited from using data in certain ways. Generally, financial institutions and insurers may not take certain adverse actions solely on the basis of an individual's past criminal record, physical condition or developmental disability, age, marital status, sexual preference, or "moral" character.

  - *It is likely that additional data security and privacy safeguards may soon be effective, including a new data security statute for the insurance industry.* Prior to the COVID-19 pandemic, the Legislature was set to approve an industry-supported, Wisconsin-specific version of the National Association of Insurance Commissioners ("NAIC") Insurance Data Security Model Law, adopted in 2017.[1] This legislation was developed through a deliberate process involving regulators, insurers, and consumer advocates, and relies on the Office of the Commissioner of Insurance's (OCI) regulatory authority. Separately, through the NAIC, state insurance regulators are also currently considering whether improvements to data privacy are appropriate. That effort may lead to further revisions within the existing regulatory structure – which could be implemented in Wisconsin for the insurance industry and others.

  - *Wisconsin's insurers and financial institutions are already subject to significant and targeted regulatory oversight of data privacy and security.* Insurance regulators take a proactive approach in monitoring insurer compliance with already-existing data security and privacy requirements. The NAIC Financial Examiner Handbook and the Market Regulation Handbook provide guidance on examining information technology controls to help ensure entities are taking reasonable and necessary steps to protect consumers from theft or loss of personal information. In addition, the federal Interagency Guidelines Establishing Information Security Standards requires financial institutions to assess the risks posed to sensitive customer information and implement procedures to protect against those risks on an ongoing basis, with boards of directors and management oversight. The Federal Financial Institutions Examination Council recently released its Cybersecurity Assessment Tool to provide a concrete framework for determining the strength of an institution's security protocols. By focusing on risk assessments and governance, the guidance allows data security practices to be developed commensurate with an institution's risk profile, without a one-size-fits-all solution, and evolve as technology changes.

[1] If the legislature convenes in July this legislation may pass. If the legislature does not convene, we expect the legislation will be approved early in the 2021-22 legislative session.

- **If action is necessary, ensure it is targeted and consistent with the existing framework.**

  - *Work only within "gaps."* If the committee believes that further action is necessary, despite the already-existing regulatory framework, it should avoid duplicating any of the above-described laws and regulations. Rather, it should clearly identify what "gap" needs to be filled and limit its actions to addressing that limited need.

  - *Identify a single license-issuing regulatory body as the exclusive regulator for insurers and financial institutions already operating under the existing framework.* As the number of regulators overseeing an industry increases, costs and uncertainty increase as well. The potential for conflicting interpretations also increases. Any marginal benefit of increased oversight by a second regulator will be of particularly little value in already highly-regulated industries like insurance and financial services, which are subject to the oversight of their respective regulators.[2] The laws and regulations governing insurers and financial institutions already balance data privacy with other important considerations, including solvency, safety and soundness, and market conduct. These regulatory agencies also possess a unique understanding of the business practices and processes within these industries.

  - *Provide exemptions to entities that are subject to the already-existing framework.* For maximum consumer clarity, the committee should specify that businesses that already comply with HIPAA, GLBA, and state counterparts do not need to comply with any new, additional regulations that may be imposed. This is the approach the current framework has adopted, consumers expect it, and it should not be changed. Indeed, the California Consumer Privacy Act ("CCPA") took this approach in large part, by exempting personal information that constitutes PHI or non-public personal information from the data privacy requirements of CCPA, and the recently proposed Wisconsin Data Privacy Act, while not ideal, included similar exemptions for those categories of data (as well as other categories subject to regulation, including data subject to FCRA). Unfortunately, merely exempting data, as opposed to entities, caused additional confusion under CCPA. We support entity-level exemptions, as opposed to complicated data-based exemptions, which are hard for consumers to understand and difficult for businesses to operationalize in practice.

III. Principle 2: Retain and expand the risk-based approach to data privacy laws.

As already described, the existing regulatory framework relies on a concept of concentric circles, with the most sensitive personal data subject to the highest level of protections and less sensitive data subject to fewer requirements. The Advisory Committee should maintain this risk-based model for data privacy and security laws because it is consistent with consumer expectations. Indeed, one of the major challenges with CCPA, because of its broad definition of "personal information," is determining what exact information is subject to the law. For instance, should a name and address – information you can easily find online – be accorded protection equal to social security numbers, credit cards, and other sensitive personal information?

Lessons can be learned from the existing opt-in/opt-out structure for health and personal financial data in INS Chapter 25, which draws a distinction between various types of data and consumers' expectations for privacy. Under current law, Wisconsin has already enacted a regulatory

[2] We have provided a copy of this communication to Commissioner of Insurance Mark Afable and Department of Financial Institutions Secretary Kathy Blumenfeld with the hope that their firsthand knowledge and experience with the data privacy and security laws may also support these efforts to develop effective, industry-specific regulations.

structure that requires explicit approval for the release of health information ("opt-in"), given its extreme sensitivity. The same regulatory structure gives consumers the ability to actively prevent financial information from being shared ("opt-out") with non-affiliated third parties, given the less significant concerns surrounding that information. In other situations, providing notice to customers of how a business may use data is appropriate.

It is important to note that obtaining consent from consumers can be incredibly difficult, especially when businesses collect personal information over the phone, in person, and online. Businesses continue to struggle with CCPA's requirement to provide notice at the time of collection, especially when collection may occur on the phone, in a restaurant, at a football game, at a convention, or other offline locales. Subjecting all classes of data to these requirements would create a scenario where consumers were being constantly inundated with privacy policies, checkboxes, pop-ups, cookie consents, browser banners, and opt-in requests. Think about the number of times you have been asked recently to agree to a "click-wrap" agreement; now imagine having to take a similar action every time you visit a website, sign up for an email list, drop your business card in a jar at a convention, or provide your credit card to pay for food. The average consumer does not desire the additional transaction friction for every potential disclosure of information.

Wisconsin's existing data breach notification law respects consumer expectations, taking a reasonable position by requiring notification to consumers only when sensitive personal information has been accessed or disclosed. CCPA includes a similarly restrictive definition of personal information with respect to data breaches, such that notifications are required only when certain sensitive information is accessed or disclosed, and not when personal information such as IP address, address, or phone number are accidentally disclosed. Both the Wisconsin and California approaches match consumer expectations, leading to disclosures only when there has been a data breach or disclosure with increased potential for actual resulting harm.

The Wisconsin Data Privacy Act ("WDPA")—which was proposed but not passed earlier this year—stands in stark contrast to Wisconsin's current scheme. It defined the term "personal data" broadly to include information such as email address. As introduced, the law would have required breach notification to consumers every time such information was disclosed to a third party unless disclosure was "unlikely to result in a risk to the rights and freedoms of consumers."

Under the WDPA, Wisconsin businesses would also be required to notify consumers if they receive a consumer's personal information from another party, even for a legitimate business purposes—like a referral.[3] These requirements in WDPA would have caused a massive influx of emails and written notices to consumers, subverting the privacy protection component of the law in favor of nuisance communications. Moreover, the WDPA would have implemented a default opt-in system for practically all data—requiring affirmative consent for businesses to process any personal information, including names and addresses, except in certain limited and vague circumstances. The WDPA's one-size-fits-all regulation of personal data is not: (a) consistent with the expectations of consumers, (b) realistic in a technology-driven world, and (c) conducive to business innovation. The WDPA fails to make any attempt to fit within the existing regulatory scheme, except for exemptions regarding certain types of information subject to other regulatory schemes.

[3] Similarly, if an insurance agent was provided the name, email address, and telephone number of a prospect from a friend, the insurance agent would need to contact the prospect and provide a disclosure about how the insurance agent received that personal information, even if the prospect provided their information for that specific purpose. A final example is worthwhile. If an attorney received an email from a client that said company ABC wanted to fire Sally, under the WDPA the attorney would need to email Sally and let her know within thirty (30) days how the attorney obtained her information—that could be a problem if Sally doesn't know she will be fired.

The WDPA also proposed fines up to $20 million dollars for violations of its provisions. This number that is guaranteed to scare off businesses of all sizes and shapes from entering Wisconsin's business community and is unnecessary to provide an incentive to financial services companies to protect consumer information. In the event consumer information is compromised, financial services companies often bear the brunt of expenses associated with the breach. For example, credit and debit card issuers may be subject to fines from the card brand associations (such as Visa and Mastercard). Depository institutions may be liable to their customers for unauthorized transactions conducted under the card brands' zero liability programs and the Electronic Funds Transfer Act and Regulation E, regardless of whether the institution was at fault. Financial services companies suffering data breaches incur the second highest per record cost of responding to and remediating a breach, behind only the healthcare industry.

Beyond hard dollar losses, financial services companies can be exposed to serious reputational harm following a breach, which can contribute to lost revenue from customer attrition. The WDPA deficiencies noted above will subject businesses to vastly greater regulatory costs and burdens if enacted. Any benefits the law could bring to consumers may be outweighed by consumer exhaustion and apathy, and the law would almost assuredly reduce the effectiveness of data breach notifications. If the committee is looking to impose additional regulations, the WDPA model is not supported, as it is overly broad without commensurate consumer benefits.

IV. Principle 3: Proceed in an incremental fashion and do not place Wisconsin businesses and consumers at a disadvantage.

We urge state policymakers to take a measured and incremental approach to data privacy and security legislation, given the potential costs to and impacts on Wisconsin businesses.

Wisconsin should not be an outlier, a likely result if the committee adopted something similar to the WDPA. Wisconsin must maintain its status as an attractive place for businesses to locate and operate. This does not need to come at the cost of consumer protection as the two values are not mutually exclusive. The WDPA would have placed Wisconsin on a "regulatory island," making the state less attractive for all businesses—even exceeding California's prohibitive CCPA. We would strongly encourage the committee to not emulate CCPA or GDPR, but learn from the mistakes that have challenged the implementation of each law, and the struggles that businesses (including many in Wisconsin) have endured in trying to comply with the new regulatory schemes.

For example, the rollout of the CCPA was flawed, involving last-minute amendments passed by the California legislature that materially changed the law. Although CCPA went into effect on January 1, 2020, the California Attorney General just released final implementing regulations for the law on June 1, 2020—six *months* after CCPA took effect. The final regulations follow the release of three previous iterations of regulations, each with vastly differing interpretations of the law. Adding a further level of uncertainty, the law is likely to be significantly altered once again by the California Privacy Rights and Enforcement Act (CPREA) ballot measure. The instability with the underlying law has meant that regulators in California have struggled to provide guidance for businesses to comply with the complex regulatory schemes. Many businesses and commentators would agree that California still does not have it right. While regulators, legislators, commentators, and attorneys try to determine what CCPA requires, businesses are expending significant resources to materially comply with an uncertain, complex, and burdensome law which includes some facially contradictory regulations.

It is our hope the committee will continue in a deliberative fashion, and not rush recommendations that may benefit from incorporating the experiences of other jurisdictions. This

includes both the procedural implementation of those new standards as well as the efficacy of regulations in meeting consumer expectations.

The work of this committee is a first step in avoiding the same implementation challenges in Wisconsin; but other lessons can also be gleaned from the CCPA and GDPR processes. One lesson to be learned from CCPA is the massive cost it has had to date on California businesses. Initial compliance costs to businesses in California from CCPA is predicted to be $55 billion according to a study commissioned by the California Attorney General's Office and the California Department of Justice.[4] Another lesson to be learned from both CCPA and GDPR is that businesses have actively withdrawn from those markets in response to their restrictive data privacy regimes[5], proving that flawed data privacy regulations can impact not only businesses forced to comply with those regulations, but the economic activity and attractiveness of Wisconsin as a business-friendly state.

Undoubtedly, data privacy and security legislation will require Wisconsin companies of all sizes to contribute significant resources to attorneys, consultants, and new software products – costs that will surely be passed on to consumers and lead to an increase in the price of products and services.

We urge the Advisory Committee to keep the costs of the regulations top-of-mind. An incremental approach, building off existing structures and the principles discussed here can defray much of that cost while providing consumers with substantial protections. This approach will also increase the likelihood that these recommendations are enacted into law in the upcoming legislative session.

V. Conclusion

In summary, we encourage the Advisory Committee to embrace the following recommendations as it continues its deliberations on these important issues:

- Promote harmonization with existing data regulatory requirements and regulatory agencies to promote a more tailored approach that avoids duplicative or potentially inconsistent requirements.

- Adopt a risk-based structure for regulation of data that appropriately balances the burden of implementation with consumer expectations for privacy and the harm that attaches from unauthorized disclosure.

---

[4] *See* Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, California Department of Justice by Berkeley Economic Advising and Research, LLC (August 2019), *available at* http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf; Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion To Get In Compliance*, CNBC (Oct. 8, 2019), *available at* https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html. The study also stated that compliance costs for the next decade could range from $467 million to over $16 billion. Most importantly, the study also found that the initial compliance cost to small businesses under 20 employees could be $50,000, $100,000 for companies up to 100 employees, $450,000 for companies up to 500 employees, and $2 million for companies over 500 employees.

[5] *See European Readers Still Blocked From Some US News Sites*, BBC News (June 26, 2018), *available at https://www.bbc.com/news/technology-44614885*; Hannah Kuchler, *US small businesses drop EU customers over new data rule*, Financial Times (May 23, 2018), *available at* https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

- Consistent with the risk-based approach, the definition of PII should be tied to some potential for harm from the disclosure. There are many innovative uses for data that benefit consumers. Recommendations of the committee should not stifle that innovation.

- Also consistent with the risk-based approach, Advisory Committee recommendations should follow existing opt-in/opt-out/disclosure structures. Different types of data should be subject to different levels of control based on the sensitivity and potential harm associated with the data.

- Proceed in an incremental fashion. Data laws are complex – ranging from breach notification to privacy to security. The Advisory Committee should avoid a one-size-fits-all omnibus piece of legislation, in favor of incremental progress, addressing a single issue at a time.

Thank you for your efforts to address these important issues. We look forward to continuing working collaboratively to develop an effective data privacy and security framework for Wisconsin residents and businesses.

Respectfully,

American Council of Life Insurers
American Property Casualty Insurance Association
Independent Insurance Agents of Wisconsin
National Association of Insurance and Financial Advisors - Wisconsin
National Association of Mutual Insurance Companies
Professional Insurance Agents of Wisconsin
Wisconsin Bankers Association
Wisconsin Council of Life Insurers
Wisconsin Credit Union League
Wisconsin Insurance Alliance

cc: Secretary-designee Randy Romanski, Department of Agriculture, Trade and Consumer Protection
Commissioner Mark Afable, Office of the Commissioner of Insurance
Secretary Kathy Blumenfeld, Department of Financial Institutions

22410356.11