EVERSHEDS SUTHERLAND

THE Committee OF Annuity Insurers
www.annuity-insurers.org

September 22, 2026

Chair Elizabeth Kelleher Dwyer (RI)
Co-Vice Chair Nathan Houdek (WI)
Co-Vice Chair Timothy Cornelius (WI)
NAIC Privacy Protections (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, Missouri 64106

Sent via email to: privacywg@naic.org

RE: Revised Model Law 672 – Full Exposure Draft

Dear Chair Dwyer and Co-Vice Chairs Houdek and Cornelius:

The Committee of Annuity Insurers (CAI or Committee)[1] appreciates the opportunity to submit the following comments to the NAIC Privacy Protections (H) Working Group (Working Group) on the Full Draft of Revised Model 672 dated July 24, 2026 (the Full Exposure Draft).

OVERVIEW

The CAI recognizes and appreciates the Working Group's tireless efforts to enhance privacy protections for consumers through a revised version of Model 672, an established and time-tested framework. While the Committee supports enhancing consumer privacy in a manner tailored to the insurance sector, the Committee respectfully submits that substantial work is still needed and meaningful revisions and clarifications to the Full Exposure Draft are necessary to ensure that the final model law is clear, workable, protects consumers and at the same time does not place insurers issuing annuity contracts at a competitive disadvantage relative to other financial services providers. Absent such revisions and clarifications, the CAI is concerned that the revised Model could inadvertently harm the very consumers it seeks to protect by limiting their access to annuity products that provide unique retirement savings benefits.

We note that key provisions of the Full Exposure Draft (particularly those discussed further below) unfortunately remain very unclear, making it extremely difficult at this juncture to assess the intended meaning and effect of the proposed revisions. In several instances, it is unclear whether proposed changes are intentional policy choices that raise significant concerns or whether they are merely the result of inadvertent drafting oversights. We respectfully submit that the Full Exposure Draft must be clarified and stakeholders must have additional meaningful opportunity to comment on a clearly articulated proposal before the revised Model is finalized. As this process continues, we strongly encourage the Working Group to provide more information on how it has assessed and responded to comments received, why it has proposed the language it has, and what it hopes to accomplish by doing so. Providing this kind of transparent communication, similar to what would be provided as part of a state or federal administrative rulemaking process, would maximize the utility and efficiency of the

[1] The Committee of Annuity Insurers is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 33 member companies represent approximately 80% of the annuity business in the United States. More information is available at https://www.annuity-insurers.org/.

process going forward and ensure that the Working Group and stakeholders are talking to each other, not past each other.

We have focused the substance of our current comments on what we believe is the intended meaning of the revisions in the Full Exposure Draft and the most critical issues they raise. As you continue to work through this process, we strongly urge you to provide stakeholders with explanations of the Working Group's thinking on key issues and fair opportunity for all stakeholders to submit comments on further proposed revisions to Model 672 based on that information .

The comments below focus on issues of particular importance that we have identified in the Full Exposure Draft. In addition, we have appended to this letter an annotated and red-lined copy of the Full Exposure Draft, which includes additional issues and clean-up that we believe need to be addressed, our reasoning, and suggested language. We hope you find these comments and suggestions constructive and helpful at this juncture.

COMMENTS

1. **The final Model framework must not leave insurers at a competitive disadvantage. Limiting the regulatory burden on insurers and preserving the ability to engage in joint marketing and compete in the broader marketplace is crucial.**

   Annuity products compete with traditional investment accounts, like bank savings accounts and mutual funds, among others. Annuity products provide unique benefits to consumers — like guaranteed income and limited downside risk — that cannot be replicated by traditional retirement savings products. Those competing products are regulated under the Gramm-Leach-Bliley Act (GLBA) through the SEC's recently updated Regulation S-P, which continues to take an opt-out approach consistent with current Model 672. Those products are not subject to privacy rules under state insurance laws. Differences in regulatory burden directly influence product development and pricing decisions and influence financial advisors' product recommendations. If revised Model 672 subjects annuity insurers to materially more limiting and burdensome standards than the standards applicable to traditional retirement savings products, it will hamstring insurers from effectively competing in the broader financial services marketplace; financial advisors would be less likely to recommend annuity products and consumers who would benefit from an annuity would be less likely to have access to them.

   While some limited opt-in (consent) requirements may be workable with appropriate exemptions in place, the best way to ensure annuity insurers can remain competitive in marketing their products to consumers who could benefit from them is by maintaining a predominantly opt-out approach consistent with current Model 672 and the GLBA. As discussed further below and in our attached markup, clarifying changes are needed to ensure that annuity insurers are not prevented from competing in the broader financial services marketplace. Above all, the Committee urges the Working Group to carefully consider any changes that may put annuity insurers at a competitive disadvantage compared to competing non-insurance retirement products. In particular, we emphasize that it is imperative that final revisions retain the existing joint marketing exemption in Section 22, which is essential to annuity insurers' ability to educate consumers and compete with non-insurance retirement products. Additionally, it is important that newly defined restrictions on the ability to disclose personal information to nonaffiliated third parties (such as the limits on sales or targeted advertising) do not act to limit the ability of annuity insurers to market their products or compete with non-insurance retirement products.

2. **The contractual requirements of Section 5 should be integrated into Section 22 to clarify how they fit into the existing Model 672 structure and to avoid creating unintended duplication or confusion.**

   As we have previously commented, mandating that all service provider contracts contain certain prescriptive provisions is a problematic approach. To the extent a licensee is unable to extract contractual terms that precisely match the requirements of Section 5, the licensee would be

effectively barred from using that service provider, regardless of whether that service provider would be the most beneficial for the licensee and its consumers overall. We suggest that it should be sufficient for licensees to remain responsible for compliance with the law, including when nonpublic personal information (NPI) is processed by service providers on their behalf.

Additionally, current Section 5 and Section 22A contain two separate and inconsistent provisions establishing contractual requirements for third-party service providers to qualify for the service provider exemption. It is also unclear whether joint marketing agreements required under Section 22 are also subject to the requirements of Section 5. This duplication and ambiguity generates confusion around how the Section 5 requirements apply. At minimum, the requirements of Section 5 should be integrated into the existing third-party service provider contracting provisions of Section 22A. More limited contractual requirements for joint marketing agreements with nonaffiliated third parties that are not third-party service providers should be separately and clearly established in Section 22B. This would better preserve the existing structure of Model 672, avoid unintended consequences that may arise from structural changes to the existing model, and clarify the distinction between the contractual requirements for third party service providers and the contractual requirements for nonaffiliated third parties that are not third-party service providers.

In addition, we urge the Working Group to provide more flexibility under Section 5 for third-party service providers to (i) respond to lawful requests by law enforcement or a governmental body without requiring a "valid and binding" order; and (ii) notify the licensee of its failure to meet any of the contractual obligations in Section 5 promptly after discovery, rather than specifying a strict and unnecessarily prescriptive 48-hour time period that would need to be uniform across all service provider contracts. Finally, Section 5B should clarify that the licensee's responsibility for "handling" NPI is limited to the NPI the licensee disclosed to the third-party service provider.

3. Licensees should not be required to disclose a list of all third-party service providers to whom the licensee has disclosed a consumer's NPI.

The proposed obligation under Section 6A(1)(b) to provide a list of all third-party service providers to whom a licensee has disclosed a consumer's NPI would be burdensome, complex, and serve little apparent consumer protection purpose.

The CAI believes that consumer disclosure obligations should provide meaningful, actionable information to the consumer rather than overwhelming them with information they cannot use and may not have requested. The list of service providers would have to be provided even if the consumer does not want and does not request the information, such as where the consumer is only interested in what NPI the licensee maintains about the consumer. It is unclear what meaningful benefit this information would provide to a requesting consumer. The average consumer has little use or interest in knowing the reinsurer, third-party administrator, managing general agent, cloud service provider, or other vendor that the licensee engages to carry out the business of insurance. Even if a consumer objected to the use of a particular third-party service provider, there is (appropriately) no right for a consumer to choose which third party service providers a licensee uses. Pursuant to the exemption for service providers under Section 22, a consumer has no right to opt out from having their NPI shared with a particular third-party service provider.

It would also be very challenging and resource intensive for licensees to track exactly which service providers have received NPI about which consumers. Different vendors may be used for different products, those vendors change over time, and some vendors may be relevant in some circumstances but not others. For example, one vendor may be used in connection with processing claims for certain products, at certain times, but not for others. Determining whether a particular consumer's data was sent to that vendor would require the licensee to determine whether that consumer filed a claim on the particular product, during the particular time frame, when it would have gone to that vendor. There are many other additional factors and circumstances that could add substantial complexity and operational difficulty to tracking exactly which service providers have received NPI about a particular consumer. Moreover, this requirement is not subject to any time

limitation and could therefore be read to require a licensee to provide lists spanning decades of third-party service providers with whom the licensee no longer has a business relationship.

Accordingly, the CAI recommends limiting this disclosure obligation to *categories* of nonaffiliated third parties to whom the licensee has disclosed the consumer's NPI in the preceding 12 months. This approach would be consistent with the general approach taken under the California Consumer Privacy Act and other state privacy laws and focus on providing actionable information to consumers, while avoiding placing a substantial burden on licensees with little corresponding benefit to consumers.

4. Exemptions from the right to deletion should be expanded to include additional important exemptions that broadly apply.

Subsection 6.C.(2) appropriately provides certain exceptions from a licensee's obligation to delete NPI in response to a consumer request, including where the licensee is required by law or regulation to retain the information. However, there are additional circumstances where it is important for licensees to be able to retain certain NPI that are not clearly covered by the existing exemptions. This provision should be clarified to permit licensees to retain and process information that is reasonably necessary for normal and expected internal operations and public interest purposes, including safety, security, and anti-fraud efforts. For example, we note that, prior to the point when a licensee reasonably anticipates a claim or civil or criminal proceeding, a licensee may need to maintain NPI for security and antifraud purposes. In the absence of such provisions, it is possible a bad actor may exploit the requirement to timely respond to requests under Section 6 to engage in fraudulent activity and seek to destroy the potential evidence thereof before the licensee is able to determine that a claim or civil or criminal proceeding might arise in connection with the NPI subject to the deletion request. Fraudsters are increasingly sophisticated in their efforts to exploit data privacy rights to facilitate their schemes, and robust exemptions for fraud prevention are essential to combat them and protect legitimate consumers. Accordingly, a broader list of exemptions should be added to broadly protect appropriate and necessary uses of NPI under a revised Model 672. This approach would be consistent with the approach and language adopted by most states that have adopted comprehensive privacy laws.

5. Data should not have to be deleted from backup systems until the backup system is restored to an active system or is next accessed in the ordinary course.

Subsection 6.C.(3) allows deletion to be delayed by up to 45 days where the data is stored on archived or backup systems. However, this 45-day limit does not account for the diverse technological and security architectures that licensees employ to protect consumer NPI or the disproportionate burden of responding to deletion requests with respect to backup or archive systems outside of the ordinary course of business. Some backup and archive systems (e.g. tape archives) are rarely accessed, and immutable backups (i.e., WORM compliant systems established to comply with SEC regulations) are by their nature designed so that they cannot be deleted as an important cybersecurity control.

Mandating deletion within a specified time period would require licensees to identify any backup or archive systems that may contain the consumer's NPI and access those systems solely for purposes of carrying out the deletion request. Not only would this add significant operational costs to licensees, but it could also increase the security risks to those backup systems by requiring that they be accessed more frequently and for different purposes than they would be accessed in the ordinary course. An essential feature of backup and archive systems is that they are appropriately segregated from production systems so that they are secure and available when production systems are lost or compromised. Immutable backups are particularly important as a defense against the risk of ransomware and similar destructive attacks, allowing the licensee to restore active systems after an attack. In recent years, insurance companies have increasingly been targeted by such attacks, and ransomware threats to the insurance sector continue to increase in both frequency and sophistication. In the absence of an exemption for these systems, the Act would essentially prohibit

immutable backups, which would place both the licensee's business operations and the consumers' NPI at greater risk.

Subsection 6.C.(3) should therefore preserve immutable backups and other appropriately segregated backup systems by allowing licensees to defer deleting data from such a system until it is restored to an active system or next accessed in the ordinary course and deletion is reasonably feasible. Doing so would still protect consumers whose data is not deleted from such systems within 45 days of the authenticated request, since any access to the system would trigger the deletion obligation and would prevent any inadvertent use or disclosure of the NPI. This approach would better balance consumer privacy risk with licensees' cybersecurity risks and operational burdens and would be consistent with the approach taken by other privacy laws, including the California Consumer Privacy Act (CCPA).

6. Licensees should be exempted from honoring requests where doing so would involve disproportionate effort.

Subsection 6.D.(1)(b) includes an exemption that excuses licensees from responding to authorized consumer requests where the request cannot be fulfilled because the specific NPI is not locatable or retrievable by the licensee. The CAI appreciates and supports the recognition within this section that in some cases a licensee may be unable to locate or retrieve certain data after trying to honor the request, and the Working Group's revision removing the previously proposed "impossible" standard to qualify for this exception is a positive development. However, this subsection would still apparently require an affirmative determination that the NPI cannot be located or retrieved before the exemption would apply. We continue to believe there should be an express exception for circumstances where locating or retrieving such information would involve disproportionate effort (e.g., if honoring a consumer's request would require hundreds of hours of manually reviewing hardcopy documents or searching through legacy systems that were not designed with modern data retrieval capabilities). Other modern privacy frameworks, including the CCPA, allow businesses to decline to honor consumer requests where doing so would involve disproportionate effort. Implementing a similar standard here would better balance the interests of consumers in exercising their privacy rights with the potential practical difficulties of honoring those requests, and would ensure that licensees' resources are focused on honoring requests that can be meaningfully fulfilled. The CAI also recommends corresponding changes to the drafting note so that examiners are directed to review the licensee's justifications for denying a consumer request under the disproportionate effort standard, including the facts and circumstances supporting the determination.

In addition, the CAI recommends removing the language indicating that there shall be no cap on the number of requests to correct or delete NPI. Affirmatively specifying that there is no cap could inadvertently encourage repetitive and abusive requests, which would divert resources from responding to legitimate consumer requests. Therefore, if a cap is not adopted, the Model should remain silent on this point. This approach is consistent with state privacy laws, which generally do not affirmatively state that there is no limit on the number of requests.

7. Article IV's expanded notice requirements should be narrowed and clarified to avoid undue operational burdens.

Under the Full Exposure Draft, the distinction between a "consumer" and a "customer" has been eliminated and, as a result, the Model requires annual privacy notices to be provided to all consumers, including former customers and consumers who never become customers. Because the obligation to provide privacy notices is no longer tied to the formation of an ongoing customer relationship, this substantially increases the operational burden and costs on licensees in providing such notices.

Licensees are generally required to retain records of contacts with consumers for several years or may retain information on backup systems for security purposes and would therefore be obligated to provide annual privacy notices during that time even if the licensee does not use or disclose the consumer's NPI for any purpose other than to meet its legal obligations or for another permitted

purpose under the Model. However, consumers that do not have an ongoing relationship with a licensee would not expect to continue receiving annual privacy notices and providing such notices may generate confusion or concern. For example, a consumer that applied for, but ultimately did not purchase, an insurance product may question why the licensee is continuing to send annual privacy notices years later. From the consumer's perspective, receiving annual privacy notices from a company with which they have no ongoing relationship may feel intrusive rather than protective and prompt unnecessary consumer inquiries or complaints. Where the consumer's NPI is retained solely to comply with a legal requirement or for a purpose otherwise expressly permitted under the Model (e.g. security or anti-fraud purposes), the licensee would also not be obligated to honor the consumer's request if the consumer submits a request for deletion in response to receiving an annual privacy notice.

Accordingly, the CAI recommends an express exception from the notice requirement be provided for consumers with whom the licensee has no ongoing relationship and where the NPI is retained solely to comply with a legal requirement or for another permitted purpose under the Model. This exception would reduce consumer confusion while appropriately focusing annual notice requirements on consumers who have a meaningful relationship with the licensee.

Additionally, Section 10 currently ties the short-form initial privacy notice to delivery of an opt-out notice. Because privacy notices are now required for all consumers, including those for whom no opt-out right would apply, it is important that Section 10 be revised to permit the use of the short-form notice broadly without necessarily requiring an accompanying opt-out notice. Enabling the use of the short-form notice also helps balance the burden placed on licensees to delivery notices to all consumers, not just those that become customers, with the interest of consumers in having access to information on how their NPI will be processed.

Finally, the elimination of the distinction between a "customer" and a "consumer" and the elimination of existing exemptions from the initial notice requirement for consumers in Section 5B of existing Model 672 has the effect of obligating a licensee to provide initial and annual notices to all consumers whose NPI the licensee received from another financial institution pursuant to a joint marketing agreement (e.g., a list of individuals to be jointly marketed to), even though the licensee's use of such consumers' NPI would be limited to the permitted purpose of conducting the joint marketing.

This result is entirely inconsistent with the nature and purpose of the joint marketing exemption and serves no practical consumer protection purpose. Requiring licensees to deliver initial and annual privacy notices to consumers on a joint marketing list – individuals who may have no awareness of or relationship with the licensee – would generate significant consumer confusion. Such notices would lack the context necessary for a consumer to understand how the licensee's information practices are meaningful to them. In addition to generating consumer confusion, this requirement would impose a substantial burden on licensees and impair insurers' ability to compete in the broader financial marketplace through joint marketing.

Accordingly, the CAI recommends a limited exemption from the requirement to provide initial and annual notices to consumers whose NPI the licensee received from a nonaffiliated third party pursuant to a joint marketing agreement, provided that the licensee provides the applicable notices when the consumer enters into an ongoing relationship (i.e., customer relationship) with the licensee and before the licensee discloses the consumer's NPI to a nonaffiliated third party other than as authorized by Sections 23 and 24. This approach would ensure that every consumer receives the full complement of initial and annual notices at the point when those notices are both relevant and actionable, while avoiding the delivery of notices that would confuse consumers and unduly burden licensees.

8. The prescribed time period for acting on an opt-out request should be extended and applied consistently.

Section 12 would require that licensees act on an opt-out request within 10 days of receipt. This directly conflicts with a parallel requirement in Section 19 which would require licensees to comply

with a consumer's opt-out direction no later than 15 days after receipt. These provisions should be aligned with one another for the avoidance of doubt. Moreover, the prescribed time period should be extended to allow 30 days for compliance, which more appropriately reflects the operational realities of implementing opt-out requests across systems and use cases. If an opt-out request is received after a licensee has already begun disclosing a consumer's NPI to nonaffiliated third parties (i.e., after the consumer was given a reasonable opportunity to exercise the opt-out right as required by Section 12), the steps the licensee must take to comply with the opt-out request may require coordination across multiple systems, product lines, and third-party relationships. A 30-day compliance period would ensure that licensees can implement opt-out requests thoroughly and completely while still requiring prompt action for consumers.

9. Article V should be revised to establish a consistent framework for when disclosure of NPI to nonaffiliated third parties is permitted, subject to an opt-out right, requires opt-in consent, or is strictly prohibited.

Section 16A(3) of the Full Exposure Draft currently appears to broadly prohibit any disclosure of NPI not specifically accounted for in the Act. While the disclosure of NPI for purposes of targeted advertising is clearly subject to an out-out right and the sale of NPI or the disclosure of sensitive personal information (SPI) each clearly require opt-in consent, it is unclear what framework applies to other disclosures of NPI not captured in these categories. Importantly, Section 16 also does not account for the Article VI exceptions. The CAI recommends establishing a default framework providing an opt-out right for any disclosure of NPI that is not allowed under the Article VI exceptions and is not otherwise expressly addressed. Doing so would continue to put meaningful control in hands of consumers, while aligning with the tried and tested default applied to financial services broadly under the GLBA. Doing so would maintain parity of insurance within the broader financial services ecosystem, while still providing consumers enhanced protections for the most sensitive types of disclosure (sale and processing SPI).

It is additionally unclear how the opt-out right for targeted advertising under Section 19 is intended to fit within the broader framework of limits on the disclosure of NPI. We suggest that this requirement should be clearly articulated as an exception to the otherwise permitted disclosure of NPI to service providers and joint marketing. We believe this is, in fact, the intent of providing the opt-out requirement specifically for targeted advertising, and doing so would provide a powerful consumer right to limit how their data is used for cross-context behavioral advertising while preserving the broad ability of licensees to engage service providers and engage in joint marketing.

10. Section 17 should be revised to clarify how licensees who receive NPI from nonaffiliated third parties that are not service providers may use or disclose that NPI.

It is currently unclear what the revisions to Section 17 are intended to accomplish. Under existing Model 672, the equivalent section functions to define how a licensee who receives NPI under any exemption in Model 672 is permitted to further use or disclose that NPI. It generally allows them to use the NPI for exempted purposes (i.e. Article VI exempted purposes) or to disclose NPI in ways that the original disclosing financial institution would have been permitted to disclose the NPI directly.

Revised Section 17 does not carry out this same function. Rather, it would appear to only apply to NPI received pursuant to the exemptions defined in Sections 20 and 21 of revised Article V, but not the exemptions provided in Article VI. Additionally, it would appear to apply only to NPI received from nonaffiliated third-party service providers, but not necessarily other financial institutions who are not service providers (e.g. NPI disclosed from a ceding insurer to a reinsurer). As the CAI previously commented, these changes strip away the framework and structure of existing Model 672 without providing a replacement framework. This leaves non-service provider disclosures apparently subject only to the general rules articulated in Section 16, creating uncertainty about how licensees should handle NPI received from other financial institutions in the ordinary course of business and lacking necessary exemptions for the normal conduct of the business of insurance.

Section 17 should be revised to apply to nonaffiliated third-party licensees regardless of whether they are service providers.

11. The definition of "third party" should be separated from the definition of "third party service provider."

The definition of "third party" has been bundled into the definition of "third party service provider." This converts references to a third party throughout the Act into references to a third-party service provider, even when the third party is clearly not a service provider. This would create numerous unintended consequences. The CAI recommends leaving "third party" undefined so that the Act can distinguish between nonaffiliated third parties generally and third-party service providers as the context requires.

12. The Article VI exceptions should apply to the proposed new opt-in requirements related to the disclosure of SPI.

As currently drafted, the Article VI exceptions would not apply to the proposed opt-in requirements in Article V. It is important that the exceptions to the opt-out requirements, which are well established and allow licensees to conduct normal operations, are equally applicable to the proposed opt-in requirements. While it appears the Working Group intended for the Article VI exceptions to apply to the limits on the use and disclosure of SPI under Section 21, which expressly cross-references to Article VI, that is not reflected in revised Article VI, which makes no reference to opt-in requirements whatsoever. Without an express reference to opt-in requirements, licensees would be unable to conduct ordinary insurance operations involving SPI without obtaining opt-in consent, such as disclosing SPI to a reinsurer or a third-party service provider. This ambiguity should be resolved by expressly applying the Article VI exceptions equally to both opt-out requirements and the opt-in requirements under Section 21.

* * *

As the Working Group continues work on the revised Model, we urge the Working Group to keep an eye toward ensuring that the revised draft ultimately provides clear and understandable standards that work as a whole and that any changes – particularly to the defined terms or to the structure of the Model – do not inadvertently disrupt other sections of the revised Model. We recognize that this is a complex and painstaking process, but the CAI remains committed to working constructively with the Working Group to develop a final Model that enhances consumer privacy protections while preserving the ability of annuity insurers to compete fairly in the marketplace and serve consumers' retirement needs.

We again want to express our appreciation for the opportunity to comment on the Full Exposure Draft. We hope that you find these comments and the attached annotated markup helpful. Please do not hesitate to contact us if you have any questions.

Respectfully submitted,

Eversheds Sutherland (US) LLP

For The Committee of Annuity Insurers

Eversheds Sutherland (US) LLP

Please direct any questions or requests regarding this letter to any of the following:

Stephen E. Roth
Partner
Eversheds Sutherland (US) LLP
SteveRoth@eversheds-sutherland.us
202.383.0158

Alexander F. L. Sand
Partner
Eversheds Sutherland (US) LLP
AlexanderF.L.Sand@eversheds-sutherland.us
512.721.2721

Mary Jane Wilson-Bilik
Partner
Eversheds Sutherland (US) LLP
MJWilson-Bilik@eversheds-sutherland.us
202.383.0660

PRIVACY OF CONSUMER INFORMATION ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose
Section 2. Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required
Section 8. Annual Notice of Information Practices to Consumers Required
Section 9. Information to be Included in Notices of Information Practices
Section 10. Short Form Initial Notice of Information Practices
Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods
Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal ~~InformationSection~~ Information
Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information
Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing
Section 23. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions
Section 24. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26. Authorizations
Section 27 Authorization Request Delivery
Section 28. Relationship to Federal Rules
Section 29. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act
Section 31. Nondiscrimination
Section 32. Violation
Section 33. Severability
Section 34. Individual Remedies
Section 35. Effective Date

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 2026 National Association of Insurance Commissioners

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B. Compliance. A licensee domiciled in this state that is in compliance with this Act in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026 National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Act, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices content requirements of this Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this Act.

Section 4. Definitions

As used in this Act, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

C. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

© 2026 National Association of Insurance Commissioners

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

D. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

E. "Commissioner" means the chief insurance regulatory official of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

© 2026 National Association of Insurance Commissioners

F. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal information about the individual to a nonaffiliated third party other than as permitted under Sections 22, 23, and 24 of this Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 7, 8, and 13 of this Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal ~~financial~~ information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections 22, 23, or 24 of this Act, such an individual is not the consumer of the licensee solely because he or she is:

Commented [ES1]: Corrected apparent typo - the term "nonpublic personal financial information" has been replaced with "nonpublic personal information" in all other instances throughout the draft.

© 2026 National Association of Insurance Commissioners

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be consumers for purposes of this Act.

Commented [ES2]: As revised, these provisions directly conflict with one another. Originally, paragraph (ii) was intended to prevent a consumer covered under paragraph (i) from being considered a customer. This needs to be clarified.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

© 2026 National Association of Insurance Commissioners

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

~~M~~M. "Genetic information" means any data, regardless of format, that: (1) results from the analysis of an individual's biological material, including analysis of the complete DNA, regions of DNA, chromosomes, genes, or gene products; and (2) concerns an individual's genetic characteristics. "Genetic information" does not include de-identified data.

Commented [ES3]: The term "genetic information" was included in the definition of "sensitive personal information" but was not, itself, defined. In order to clarify the scope of "sensitive personal information," the CAI proposes this definition, which we note is consistent with the definition used in the privacy laws of Indiana, Connecticut, and other states.

N. "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

© 2026 National Association of Insurance Commissioners

~~N~~O. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice, opt in and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

~~(a)~~ ~~The~~(a) To the best of the licensee's knowledge, the principal otherwise complies with, and provides the notices required by, the provisions of this Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22 of this Act, except as permitted by Section 23 or 24 of this Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES
"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

~~O~~P. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

Commented [ES4]: It is important that these exemptions extend to opt in requirements, not just notice and opt out requirements. We believe this was an inadvertent omission.

Commented [ES5]: We note that a licensee should not be made subject to the notice and opt out requirements by virtue of the principal's failure to comply with and provide notices under the Act if it reasonably believed the principal was in compliance and had provided such notices.

© 2026 National Association of Insurance Commissioners

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

~~P~~O. "Nonpublic personal health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

~~Q~~R. "Nonpublic personal information" means any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

Formatted: Indent: Left: 1"

~~R~~S. (1) "Personally identifiable information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers

© 2026 National Association of Insurance Commissioners

or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable information does not include:

Formatted: Indent: Left: 1", First line: 0.5"

(i) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

~~S~~T. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

~~T~~U. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22, 23, or 24.

~~U~~V. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

© 2026 National Association of Insurance Commissioners

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

~~V~~W. "Reasonable opportunity" means any of the following:

(1) The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time; or

(3) For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. "Sale" or "selling" means the exchange of nonpublic personal information with a nonaffiliated third party for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

Commented [ES6]: The definition of "sale" or "selling" should be clarified to exclude affiliates. Without this clarification, affiliates may share information systems or otherwise have access to nonpublic personal information in a way that may be viewed as involving monetary or other valuable consideration.

© 2026 National Association of Insurance Commissioners

(2) A licensee provides information to or receives anything of value from an insurance support organization, statistical agent, or reinsurer;

(3) A licensee provides nonpublic personal information to ~~an affiliate or to~~ a ~~financial institution~~nonaffiliated third party with which the licensee performs joint marketing;

(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means ~~personally identifiable~~ "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information ~~or~~and biometric data that ~~may be~~is processed for the purpose of uniquely identifying an individual.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on nonpublic personal ~~data~~information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing Nonpublic Personal Information solely for measuring or reporting advertising performance, reach, or frequency.

AA. "Third party service provider" ~~or "third party"~~ means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

Commented [ES7]: This language suggests that joint marketing limitations apply to marketing with affiliates, however the joint marketing provision (Section 22) only applies to disclosures of information with nonaffiliated third parties. This should be clarified.

Commented [ES8]: "Personally identifiable" is included in the definition of "nonpublic personal information" and therefore this language is duplicative and should be deleted.

Commented [ES9]: Consistent with the recommendation to define the term "genetic information," we recommend changing "or" to "and."

Commented [ES10]: Updated for consistency with the definition of the term "biometric data," which only includes such data that is "used to identify a specific individual." The term "may" implies a deviation from that definition for purposes of "sensitive personal information" which does not appear to be intentional.

Commented [ES11]: The term "personal data" is not defined, which raises questions regarding the scope of "targeted advertising." In keeping with the scope of the Act as described in Section 2, we recommend using the defined term "nonpublic personal information" here.

Commented [ES12]: Providing that the term "third party" has the same meaning as the term "third party service provider" essentially results in all references to third parties throughout the Act referring exclusively to service providers and leaves no means of describing third parties that are not service providers. This creates a range of confusing and, we believe, unintentional outcomes.

© 2026 National Association of Insurance Commissioners

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes, unless processing is necessary to comply with the law or a ~~valid and binding order of~~ lawful request by law enforcement or a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above ~~within 48 hours of~~promptly after discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of such nonpublic personal information.

Commented [ES13]: As discussed in CAI Comment #2, this section is duplicative and confusing in connection with Section 22A. Our changes are intended to align the two sections. See corresponding suggested edits in Section 22.

Commented [ES14]: The Working Group should consider providing more flexibility for third party service providers to respond to lawful requests by law enforcement or a governmental body without necessarily requiring a valid and binding order.

Commented [ES15]: The Working Group should consider adopting a less prescriptive standard for the timing of notification. For example, if a service provider refuses to commit to anything less than 72 hours (a common industry benchmark), that should not lead to a violation of this Section 5.

Commented [ES16]: This change is intended to clarify that the responsibility for handling nonpublic personal information specifically relates to nonpublic personal information disclosed to the third party service provider by the licensee.

© 2026 National Association of Insurance Commissioners

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of ~~all~~the categories of nonaffiliated third ~~party service providers~~ parties to whom the licensee disclosed the consumer's nonpublic personal information in the preceding 12 months.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, genetic information, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information that has already been disclosed in response to the consumer's request, if it is described in a manner reasonably understandable by the consumer and the ~~consumer is offered an opportunity~~licensee takes reasonable steps to ~~review~~ensure the duplicative nonpublic personal information ~~for inconsistencies~~is consistent with disclosed nonpublic personal information; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

Commented [ES17]: As discussed in CAI Comment #3, it would be very difficult to track all third party service providers with whom a particular individual's information has been disclosed, and it is unclear what value this information would provides to consumers, considering they cannot opt out of information sharing with third party service providers pursuant so Section 22. It is also important this requirement be bounded to a reasonable time frame, such as in the past 12 months.

Commented [ES18]: Although genetic information would likely fall within the scope of "other information that could create a high risk of identity theft," we recommend expressly including it in the list of types of nonpublic personal information exempted from disclosure, given the high risk of identity theft inherent to genetic information.

Formatted: Not Expanded by / Condensed by

Commented [ES19]: Revised to clarify that "duplicative nonpublic personal information" refers to information that may be stored in multiple instances, one instance of which has already been disclosed in response to the consumer's request. In addition, this subsection implies that consumers have a secondary right to further have the duplicative information provided, which appears to negate the purpose of the exception for duplicative nonpublic personal information. Rather than providing secondary disclosure rights to duplicative information, we recommend that the exception require the licensee to take reasonable steps to ensure sets of duplicative nonpublic personal information are consistent with one another.

© 2026 National Association of Insurance Commissioners

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

(b) Delete the nonpublic personal information in dispute; or

(c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) ~~The~~The licensee reasonably determines that the nonpublic personal information is accurate and complete and ~~if the licensee~~ provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect.

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The nonpublic personal information is necessary to comply with a legal obligation; ~~or~~

(d) The nonpublic personal information is maintained in reasonable anticipation of a claim or civil or criminal proceeding~~.~~:

(e) The nonpublic personal information is maintained for purposes reasonably related to the prevention, detection, protection against, or response to security

Commented [ES20]: This provision should allow for a licensee's reasonable determination that the nonpublic personal information is accurate and complete, rather than whether such information is actually accurate.

Formatted: Font: Calibri

Formatted: Character scale: 100%, Not Expanded by / Condensed by

Formatted: Justified, Right: 0.1", Don't allow hanging punctuation, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Commented [ES21]: Replaced "information" with "nonpublic personal information" for consistency.

© 2026 National Association of Insurance Commissioners

incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; or

(f) The nonpublic personal information is maintained to the extent it may be necessary to preserve the integrity or security of systems or to investigate, report, or prosecute those responsible for breaches of system security.

(3) A licensee may delay fulfilling a consumer's request~~, up to 45 days,~~ to delete nonpublic personal information stored on an archived or backup system~~. A licensee must notify the consumer of such delay.~~ until that system is restored to an active system or is next accessed in the ordinary course and targeted deletion on the backup system is reasonably feasible, whichever occurs first.

D. Request and Response Procedures

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee or doing so would involve disproportionate effort; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for ~~irretrievability~~denying a

Commented [ES22]: As discussed in CAI Comment #4, additional important exemptions to the right to deletion should apply, particularly to safeguard necessary security and antifraud purposes.

Commented [ES23]: As discussed in CAI Comment #5, it is crucial that there be an allowance for deletion from backup systems that is not time-specific and limited where deletion is not feasible. Immutable backups are designed so that they cannot be deleted as an important cybersecurity control, and other backup or archive systems are so rarely accessed that the burden of doing so solely to delete a consumer's nonpublic personal information would outweigh the benefit of having such data deleted on the backup system while exposing the backup system to elevated cybersecurity risks.

Commented [ES24]: As discussed in CAI Comment #6, although we appreciate the revision removing the "impossible" standard, we note that this provision may still be read as requiring an affirmative determination that the nonpublic personal information at issue cannot be located or retrieved. We continue to believe allowance should be made for circumstances where locating or retrieving such information would involve disproportionate effort (e.g., if honoring a consumer request would require hundreds of hours of manually reviewing hardcopy documents). We have also made a corresponding change to the drafting note encouraging examiners to review the licensee's justifications for denying a request.

© 2026 National Association of Insurance Commissioners

consumer request under this Subsection D(1)(b)(i) during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

~~(2) There shall be no cap on the number of requests to correct or delete nonpublic personal information.~~

~~(3~~(2) If a consumer disagrees with a licensee's refusal to correct ~~or delete~~ nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:

(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

Commented [ES25]: It does not appear necessary to expressly state that there is no cap on the number of requests that may be made. Moreover, including this provision may inadvertently encourage repetitive and abusive requests.

Commented [ES26]: We note that filing a statement of disagreement is only relevant to correction requests, as the statement of disagreement provides the consumer with the opportunity to assert the information the consumer believes to be correct, relevant or fair. Accordingly, this provision should not be extended to deletion requests.

Formatted: Indent: Left: 1.5"

© 2026 National Association of Insurance Commissioners

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required

A. Initial Delivery of Notice. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal information would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13, that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

D.

Section 8. Annual Notice of Information Practices to Consumers Required

© 2026 National Association of Insurance Commissioners

A. General rule. A licensee shall provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices at least once in any period of twelve (12) consecutive months. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer on a consistent basis.

~~A.~~ Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer by December 31 of year 2.

B. Exceptions.

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 22, 23, or 24 and has not changed its policies and practices with regard to disclosing ~~Nonpublic Personal Information~~nonpublic personal information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or ~~Section~~Sections 7 or 13 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

~~(2~~(3) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

(4) A licensee is not required to provide notice to consumers with whom the licensee has no ongoing relationship, provided the licensee retains the consumer's nonpublic personal information solely to comply with a legal requirement or for purposes otherwise specifically permitted by this Act, including for security and anti-fraud purposes.

Commented [ES27]: Established the general rule as Subsection "A" for consistency with the structure of other sections of the Act.

Commented [ES28]: Converted to lowercase for consistency.

Commented [ES29]: It appears the revised notice of information practices under Section 13 was inadvertently omitted here.

Commented [ES30]: Corrected numbering.

Formatted: Indent: Hanging: 0.5", Right: 0.11", Space Before: 0.05 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Commented [ES31]: The CAI strongly urges the PPWG to adopt a limited exception to the annual notice requirement. The shift to the term "consumer" has significantly expanded the scope of this requirement without providing exceptions for circumstances where there is little value in providing an annual notice. A licensee should not be required to provide an annual notice to a consumer whose nonpublic personal information is retained only to comply with legal obligation, such as where the consumer made inquiries but never purchased a financial product or service and has no other connection to or engagement with the licensee. Additionally, notice should not be required where data is retained solely for expressly permitted uses, such as security and anti-fraud purposes.

© 2026 National Association of Insurance Commissioners

Section 9. Information to be Included in Notices of Information Practices

A. General rule. The initial, annual and revised Notice of Information Practices that a licensee provides under Sections 7, 8, and 13 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its Notice of Information Practices:

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

(2) The categories of nonpublic personal information that the licensee discloses~~,~~ to entities described in Subsection (A)(3), including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections 22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(4) An explanation of the consumer's right under ~~Section 12~~Sections 16 and 19 to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of nonpublic personal information about the consumer ~~as established under this Act~~pursuant to Section 6 and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses~~; and~~.

Commented [ES32]: This change is intended to clarify the scope of this subsection.

Commented [ES33]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. Accordingly, we recommend revising this subsection to refer to opt out rights provided under Section 16 (as set forth in our edits thereto) and 19 (providing for opt out from targeted advertising).

Commented [ES34]: For consistency with the other subsections, we recommend referring to the specific section that provides the consumer rights to request access, correction, or deletion of nonpublic personal information, rather than a general reference to the Act in its entirety.

© 2026 National Association of Insurance Commissioners

(~~c~~9) Any disclosure that the licensee makes as authorized under Section 22, 23, or 24, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections 7 and 8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. ~~Exceptions:~~

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under ~~Sections22~~Sections 22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) ~~and~~through A(8) and Subsection B of this section.

Commented [ES35]: The indentation of subsection (8)(c) appears to be in error, as it does not relate to the details of the licensee's policies and practices for protecting the confidentiality and security of nonpublic personal information that should be described. This subsection should instead be subsection (9).

Commented [ES36]: Title is not descriptive of the content of Subsection C, as Subsection C does not provide for an exception to the preceding required contents of a notice of information practices. Accordingly, we recommend removing the title of Subsection C.

Commented [ES37]: Apparent typo; it appears this was intended to refer to Subsections A(1) "through" A(8).

© 2026 National Association of Insurance Commissioners

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms ~~are~~ included in Appendix A and Appendix B, of this Act.

Commented [ES38]: Corrected grammatical error.

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices ~~at the same time the licensee delivers an opt-out notice as required in Section 12 if:~~ if:

Commented [ES39]: We note that this Subsection A assumes that an opt out notice must always be provided. This appears to have been inadvertently carried over from current Model 672, under which a notice of information practices is only required prior to forming a customer relationship where an opt out right would also be required. As revised, the notice of information practices is no longer triggered by the formation of a customer relationship where an opt out would also be required. Our recommended edit clarifies that a short-form privacy notice may satisfy notice requirements under Sections 7A and 13A even where the licensee has no obligation to provide an opt out notice because there is no applicable opt out right under the Act.

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to ~~or~~, correction, or deletion of their nonpublic personal information.

Commented [ES40]: It appears the right to request deletion of nonpublic personal information was inadvertently omitted. For consistency, we recommend including all of the consumer rights established under Section 6.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

© 2026 National Association of Insurance Commissioners

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods

A. If a licensee is required to provide an opt-~~int~~in notice under Sections 20 or 21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use. The notice shall state:

(1) The licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(2) The consumer has the option to opt in to that disclosure; and

(3) A reasonable means by which the consumer may exercise the option to opt in.

B. The licensee shall not disclose that nonpublic personal information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer. The licensee shall comply with such revocation as soon as reasonably practicable after the licensee receives it.

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it

Commented [ES41]: Corrected typo.

Commented [ES42]: Revised for consistency.

Commented [ES43]: This sentence has been added to prevent uncertainty regarding the timing for compliance with the revocation of an opt-in election.

© 2026 National Association of Insurance Commissioners

discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section 9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt-out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

© 2026 National Association of Insurance Commissioners

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than ~~10~~30 days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Commented [ES44]: We note that this 10-day time period for compliance with an opt out request conflicts with the 15-day time period set forth in Section 19 for compliance with opt out requests for disclosure of nonpublic personal information for purposes of targeted advertising. We recommend extending this time period to 30 days, which more appropriately reflects the operational realities of implementing opt-out requests across systems and use cases. At a minimum, the prescribed time period for compliance with opt out requests should be consistent throughout.

Section 13. Revised Notice of Information Practices

A. Except as otherwise authorized in this Act, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 19, 20 and 21, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal information to any nonaffiliated third party; or

(b) Discloses nonpublic personal information to a new category of nonaffiliated third party.

(2) A revised notice is not required if the licensee discloses nonpublic personal information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

© 2026 National Association of Insurance Commissioners

Section 14. Notice of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices directly to covered individuals described in Section ~~4G)~~4(G)(2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections 7 through 13 of this Act, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15. Delivery

A. A licensee shall provide any notices that this Act requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, electronically.

B. (1) A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

© 2026 National Association of Insurance Commissioners

(b) Sends the notice via electronic mail to a consumer who does not otherwise communicate with the licensee electronically.

C. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's Notice of Information Practices if:

(1) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The consumer has requested that the licensee refrain from sending any information regarding the consumer relationship, and the licensee's current privacy notice remains available to the consumer upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

© 2026 National Association of Insurance Commissioners

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information, including sensitive personal information, about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information ~~with~~, including sensitive personal information, to affiliates, provided the affiliates' use and disclosure comply with this Act.

~~(3~~(3) (a) Except as provided by Subsection A(3)(b) below, a licensee may disclose a consumer's nonpublic personal information to a nonaffiliated third party only for those purposes and uses identified in Article VI and as expressly permitted or required by Articles V or VI of this Act.

(b) Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A(3)(a) above, a licensee shall provide a clear and conspicuous notice and a reasonable opportunity to opt out of such disclosure in accordance with the requirements of Section 12.

(4) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except ~~as permitted by~~in compliance with this Act.

(~~4~~5) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under ~~Section~~ Sections 16A(3) and 19 or an opt-in right under Sections 20 and 21~~(5~~.

(6) If a consumer submits an opt-out request ~~during~~before a transaction ~~and~~is processed and disclosure of the ~~requested~~nonpublic personal information subject to the opt-out request is necessary to ~~complete~~process that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without ~~the~~disclosure of the nonpublic personal information; and

(b) Confirm whether the consumer wishes to proceed with the transaction.

B. Limits on Disclosure**.** Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details, as relevant:

(a) The consumer's right to opt out of disclosure of nonpublic personal information under Section 16A(3);

Commented [ES45]: For the avoidance of doubt given the restrictive language in Section 21, added specific references to sensitive personal information.

Commented [ES46]: Corrected apparent typo.

Commented [ES47]: As discussed in CAI Comment #9, Article V expressly provides for an opt-out requirement for the disclosure of nonpublic personal information for purposes of targeted advertising and an opt-in requirement for the sale of nonpublic personal information and the disclosure of sensitive personal information, respectively. However, it does not establish a clear baseline for the treatment of disclosures that do not fall into those categories. The following subsection could be read as a broad prohibition on any disclosure that is not expressly permitted in the Act, thereby restricting any disclosures that are not specifically addressed. It also results in uncertainty as to whether the exceptions provided in Article VI constitute "permitted" disclosure, given that they are not addressed in Section 16. We recommend this addition so that all disclosures of nonpublic personal information to nonaffiliated third parties have been addressed with an established standard of treatment, using the opt-out framework as the baseline for disclosures that are not permitted under the exceptions in Article VI or expressly required to use a specific framework under Article V (e.g., Sections 19 through 21). Corresponding changes to the following subsection clarify that disclosure of nonpublic personal information to a nonaffiliated party other than in compliance with the Act is strictly prohibited.

Commented [ES48]: We note that the only opt-out right expressly provided relates to the disclosure of nonpublic personal information for purposes of targeted advertising. It is unclear in what circumstance the processing of a transaction would require the disclosure of nonpublic personal information for purposes of targeted advertising. We have revised the language consistent with our recommendation in Section 16A(3) above. In addition, we note that it may be administratively impossible to halt a transaction to resolve a conflict with an opt-out request received "during" the transaction. Accordingly, we have revised this subsection to require confirmation to proceed with the transaction if (i) an opt-out request is received before the transaction is processed, and (ii) the transaction would require disclosure of nonpublic personal information subject to the opt out request.

Commented [ES49]: Revised to clarify that only the relevant disclosures must be made. As drafted, Section 16(B)(2) could be read to require that a consumer be notified of all possible opt out or opt in rights, even if the licensee is only providing an opt out or seeking an opt in.

Commented [ES50]: Consistent with our comment above, there should be a baseline opt-out requirement for disclosure of nonpublic personal information that does not fall within an exception in Article VI and for which there is no other express requirement articulated under Article V.

© 2026 National Association of Insurance Commissioners

(b) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(~~b~~c) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; and/or

(~~c~~d) The consumer's option to opt in to the disclosure of sensitive personal information under Section 21.

(3) Provide a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, for the consumer to exercise any applicable opt-out right ~~before disclosure~~; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

C. A licensee may allow a consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to exercise any applicable opt out right or opt in option.

Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information

A. If a licensee receives nonpublic personal information from a nonaffiliated third-party ~~service provider~~licensee under an exception in Article VI of this Act, the licensee may use and disclose the information in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

B. (1) If a licensee receives nonpublic personal information from a nonaffiliated third-party ~~service provider~~ licensee other than under an exception in Article VI of this Act, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) Affiliates of the nonaffiliated third party ~~service provider~~licensee from which the licensee received the information; and

(b) Affiliates of the licensee who may disclose the information only to the extent that the disclosure would be permissible by the licensee pursuant to this Act.

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party ~~service provider~~licensee outside of the exceptions in Article VI:

(a) The licensee may use that list for its own purposes consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party ~~service provider~~ only as permitted by this Act.

C. If a licensee discloses nonpublic personal information to a nonaffiliated third-party ~~service provider~~licensee under an exception in ~~S~~Article VI of this Act, the nonaffiliated third party ~~service provider~~licensee:

(1) May disclose the information to the licensee's affiliates; and

Commented [ES51]: Revised to clarify that one or more notices may apply.

Commented [ES52]: Corrected apparent omitted word consistent with the preceding items.

Commented [ES53]: Revised wording to clarify that the word "right" is intended to refer to the consumer's "opt-out right," rather than to impose timing of the reasonable opportunity "right before" disclosure (which would conflict with the definition of "reasonable opportunity").

Commented [ES54]: For the avoidance of doubt, we recommend including language expressly permitting targeted opt in or opt out elections, if the licensee wishes to provide that option to its consumers.

Commented [ES55]: As discussed in CAI Comment #10, this section should not be limited to the redisclosure and reuse of nonpublic personal information as between the licensee and its third party service providers. The governance of a third party service provider's use and disclosure of nonpublic personal information has already been addressed in the contractual requirements of Section 5 and the general rule of Section 16 above. This Section 17 should address limitations on the redisclosure and reuse of nonpublic personal information by nonaffiliated third parties that are themselves licensees but may not be service providers (e.g., as between a ceding insurer and a reinsurer) to align with the apparent intent of this section. Consistent changes have been made throughout Section 17.

Commented [ES56]: Corrected apparent typo.

© 2026 National Association of Insurance Commissioners

(2) May disclose and use the information in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. If a licensee discloses nonpublic personal information to a nonaffiliated third-party ~~service provider~~licensee other than under an exception in Article VI of this Act, the nonaffiliated third-party ~~service provider~~licensee may disclose the information only:

(1) To the licensee's affiliates who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

(2) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

© 2026 National Association of Insurance Commissioners

Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes

A. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer when the consumer enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising

~~A. Except as otherwise authorized in this Act~~A. Notwithstanding the provisions of Section 22, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within ~~15~~30 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt out for twelve months.

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

Commented [ES57]: Consistent with our recommended changes to the structure of Section 16 above, the disclosure of nonpublic personal information for purposes of targeted advertising in Section 19 should be treated as an exception to the service provider and joint marketing exceptions in Section 22. In other words, although service providers and joint marketing are excepted from the opt-out requirements, disclosure for purposes of targeted advertising would still be subject to an out-out right.

Commented [ES58]: We note that this 15-day time period for compliance with an opt out request conflicts with the 10-day time period set forth in Section 12 for compliance with opt out requests. We recommend extending this time period to 30 days, which more appropriately reflects the operational realities of implementing opt-out requests across systems and use cases. At a minimum, the prescribed time period for compliance with opt out requests should be consistent throughout.

© 2026 National Association of Insurance Commissioners

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in ~~subsection~~Subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

Commented [ES59]: Despite the express reference to Article VI in this section, the exceptions under Article VI remain limited to the notice and opt-out requirements — Article VI was not revised to include any exceptions to opt-in requirements as requested by the CAI. Therefore, it appears the exceptions for disclosure of SPI would be limited to those in Section 16: (i) to process a business transaction requested or authorized by the consumer; and (ii) to affiliates if their use and disclosure comply with the Act. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing nonaffiliated third party service providers to, for example, access SPI outside of the context of processing a business transaction requested or authorized by the consumer (e.g., to investigate security incidents, in connection with a merger or similar corporate transaction, etc.).

Commented [ES60]: Capitalized for consistency.

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Notice, Opt-Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections ~~12~~16A(3) and ~~19~~the opt-in requirements in Section 21 do not apply when a licensee provides nonpublic personal information to a ~~nonaffiliated~~ third party ~~to perform services for the licensee or functions on the licensee's behalf~~service provider, if the licensee:

(a) Provides the initial notice in accordance with Section7; and

(b) Enters into a contractual agreement with the third party ~~that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes~~service provider in accordance with Section 5.

~~(2) Example. If a licensee discloses nonpublic personal information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in Sections 23 or 24 in the ordinary course of business to carry out that joint marketing.~~

~~B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include~~

B. Joint marketing.

(1) The opt-out requirements in Sections 16A(3) and the opt-in requirements in Section 21 do not apply when a licensee provides nonpublic personal information to a nonaffiliated third party for the marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions~~.~~, if the licensee:

(a) Provides the initial notice in accordance with Section 7; and

() Enters into a contractual agreement with the nonaffiliated third party that prohibits the nonaffiliated third party from disclosing or using the nonpublic personal information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes.

Commented [ES61]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. We have replaced this reference with a reference to our proposed additional opt-out requirements in Section 16A(3).

Commented [ES62]: As discussed in CAI Comment #12, the exception for disclosure of nonpublic personal information for service providers should also provide for an exception to the opt-in requirement for disclosure of sensitive personal information in Section 21. Despite the express reference to Article VI in Section 21, the exceptions under Article VI remained limited to the notice and opt-out requirements — not opt-in requirements. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing nonaffiliated third party service providers to access sensitive personal information outside of the context of processing a business transaction requested or authorized by the consumer.

Formatted: Justified, Indent: Left: 1", No widow/orphan control

Commented [ES63]: Revised to clarify the contractual requirements applicable to joint marketing agreements with nonaffiliated third parties that are not third party service providers and to resolve potential conflicts with new Section 5 for third party service providers.

© 2026 National Association of Insurance Commissioners

(2) The initial notice requirements of Section 7 and annual notice requirements of Section 8 do not apply where a licensee receives nonpublic personal information from a nonaffiliated third party pursuant to a joint agreement, provided the licensee:

(a) shall provide an initial notice to a consumer in accordance with Section 7 and annual notices in accordance with Section 8 where a consumer whose information received pursuant to a joint agreement enters into an ongoing relationship with the licensee; and

(b) shall provide an initial notice to a consumer in accordance with Section 7 before the licensee discloses any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by Sections 23 and 24.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23. Exceptions to Notice, Opt-In, and Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 7A~~(2)~~, the opt-out requirements in Sections ~~12~~16A(3) and 19, the opt-in requirements in Section 21, and service providers and joint marketing in Section 22 do not apply if the licensee discloses nonpublic personal information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

Commented [ES64]: This addition accounts for the elimination of the distinction between a "customer" and a "consumer" and the elimination of existing exemptions from the initial notice requirement for consumers in Section 5B of existing Model 672.

Without this added limited exception to the notice requirements, a licensee who *receives* NPI from another financial institution pursuant to a joint marketing agreement (such as a list of individuals to be jointly marketed to) would be obligated to provide initial and annual notices to all such consumers, despite being limited in their use of the consumer's NPI to only the limited and permitted purpose of conducting the joint marketing. Such an outcome would be entirely inconsistent with the nature of the joint marketing exemption, would cause significant consumer confusion, and would be burdensome for licensees and impair their ability to compete in the broader financial marketplace.

The suggested limited exemption would avoid the need to provide initial and annual notices solely related to joint marketing, but would be clear that such notices would be required when an ongoing relationship (i.e. customer relationship) is formed or prior to disclosure of NPI to other nonaffiliated third parties except as authorized under Sections 23 and 24.

Commented [ES65]: As noted above, it is important that these exemptions extend to opt-in requirements as well as opt-out to avoid conflicting with the necessary processing or servicing of transactions.

Commented [ES66]: This provision should apply to the entirety of Section 7A, not just Subsection 2 thereof. The reference to Subsection 2 appears to have been carried over from current Model 672, which distinguished between customers and consumers. Since this distinction has been removed, this cross-reference should apply to all of Section 7A.

Commented [ES67]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. We have replaced this reference with a reference to our proposed additional opt-out requirements in Section 16A(3).

Commented [ES68]: As discussed in CAI Comment #12, the exception for disclosure of nonpublic personal information for processing and servicing transactions should also provide for an exception to the opt-in requirement for disclosure of sensitive personal information in Section 21. Despite the express reference to Article VI in Section 21, the exceptions under Article VI remained limited to the notice and opt-out requirements — not opt-in requirements. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing disclosure of sensitive personal information as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer or in connection with the circumstances specified in this Section 23.

© 2026 National Association of Insurance Commissioners

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

© 2026 National Association of Insurance Commissioners

Section 24. Other Exceptions to Notice, Opt-In, and Opt-Out Requirements for Disclosure of Nonpublic Personal Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 7A~~(2),~~ the opt-out requirements in Sections ~~12~~16A(3) and 19, the opt-in requirements in Section 21, and service providers and joint marketing in Section 22 do not apply when a licensee discloses nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

Commented [ES69]: This provision should apply to the entirety of Section 7A, not just Subsection 2 thereof. The reference to Subsection 2 appears to have been carried over from current Model 672, which distinguished between customers and consumers. Since this distinction has been removed, this cross-reference should apply to all of Section 7A.

Commented [ES70]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. We have replaced this reference with a reference to our proposed additional opt-out requirements in Section 16A(3).

Commented [ES71]: As discussed in CAI Comment #12, the other exceptions for disclosure of nonpublic personal information in this Section 24 should also provide for an exception to the opt-in requirement for disclosure of sensitive personal information in Section 21. Despite the express reference to Article VI in Section 21, the exceptions under Article VI remained limited to the notice and opt-out requirements — not opt-in requirements. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing disclosure of sensitive personal information as necessary for the critical operational needs provided in this Section 24, such as to protect against fraud; to prevent, detect, and investigate security incidents; and to comply with legal obligations.

© 2026 National Association of Insurance Commissioners

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 12F.

Drafting Note: Because the notice requirements of this Act could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this Act.

© 2026 National Association of Insurance Commissioners

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer unless an authorization is obtained from the consumer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

(1) Claims administration any processing;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

© 2026 National Association of Insurance Commissioners

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

© 2026 National Association of Insurance Commissioners

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section 26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature, including electronic signatures, of the consumer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

© 2026 National Association of Insurance Commissioners

Section 27. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer as part of an opt-out notice pursuant to Section 12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 25A.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts.

Section 29. Relationship to State Laws

Nothing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy.

© 2026 National Association of Insurance Commissioners

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act

Nothing in this Act shall be construed to modify, limit or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made regarding whether information is transaction or experience information under Section 603 of that Act.

Section 31. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer because that consumer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of this Act.

B. A licensee shall not unfairly discriminate against a consumer because that consumer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Act.

Section 32. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 33. Severability

If any section or portion of a section of this Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 35. Effective Date

A. Effective date. This ~~Acthas~~Act has been effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments to this Act, the commissioner has extended the time for compliance with the amendments to this Act until [Insert Compliance Date].

B. By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act.

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date], a contract that a licensee has entered into with a ~~nonaffiliated~~ third party ~~to perform services for the licensee or functions on the licensee's behalf~~service provider satisfies the provisions of Section ~~22A(1)(b)~~5 of this Act, even if the contract does not include ~~a requirement that the third party maintain the confidentiality of nonpublic personal information~~the provisions specified in Section 5, as long as

Formatted: Indent: Left: 1", Hanging: 0.5"

© 2026 National Association of Insurance Commissioners

the licensee entered into the agreement on or before [Insert Compliance Date].

Commented [ES72]: Revised for consistency with the contractual requirements in Section 5 above for third party service providers.

© 2026 National Association of Insurance Commissioners

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section 9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections 9A(2) and (3) to describe the

© 2026 National Association of Insurance Commissioners

categories of nonpublic personal information the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections 23 and 24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];

Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and

Others, such as [provide illustrative examples, such as "non-profit organizations"].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section 9A(2) related to the exception for service providers and joint marketers in Section 22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your

© 2026 National Association of Insurance Commissioners

creditworthiness and credit history"].

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

© 2026 National Association of Insurance Commissioners

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee", including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections 9and 11 of the NAIC *Privacy of Consumer ~~InformationAct~~Information Act*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026 National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

© 2026 National Association of Insurance Commissioners

history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections 23 and 24 of NAIC model *Privacy of Consumer ~~InformationAct~~Information Act*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an

© 2026 National Association of Insurance Commissioners

affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer Information Act*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections 11 and 16(B) of NAIC *Privacy of Consumer Information Act*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section

© 2026 National Association of Insurance Commissioners

603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section 16(B) of NAIC *Privacy of Consumer ~~InformationAct~~Information Act*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section 15(E) of NAIC model *Privacy of Consumer Information Act*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to

© 2026 National Association of Insurance Commissioners

safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section 9(A)(3) of NAIC *Privacy of Consumer Information Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section 9~~)~~(A)(3) of NAIC *Privacy of Consumer ~~InformationAct~~Information Act*], where [nonaffiliate information] appears, the licensee must:

© 2026 National Association of Insurance Commissioners

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026 National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	WHAT DOES [Name of Licensee] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	WHAT DOES **[NAME OF LICENSEE]** DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026 National Association of Insurance Commissioners

Page 2

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

© 2026 National Association of Insurance Commissioners

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

© 2026 National Association of Insurance Commissioners

EVERSHEDS SUTHERLAND

From: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
Sent: Thursday, September 17, 2026 9:58 AM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: mjwilson-bilik@eversheds-sutherland.com; Roth, Stephen <SteveRoth@eversheds-sutherland.us>; Graves, Timothy <TimothyGraves@eversheds-sutherland.us>
Subject: Draft CAI Comment Letter and Markup of NAIC Full Draft of Revised Model 672

Dear CAI Cyber & Privacy Working Group members,

We are following up on our September 9 meeting, during which we discussed possible areas for comment on the NAIC Privacy Protections (H) Working Group (PPWG)'s full draft of revised Model #672 (Full Revised Draft). As discussed on the call, we have prepared the attached draft CAI comment letter and redlined and annotated copy of the Full Revised Draft addressing the issues discussed. ***Comments are due on Tuesday, September 22. If you can provide us with any comments and reactions to the draft CAI comment letter and redline by Noon on Monday, September 21, that would be much appreciated.***

Please feel free to reach out to Steve Roth (202-383-0158), Mary Jane Wilson-Bilik (202-383-0660) or me with questions or comments.

Best,

Al
Alexander F. L. Sand | Partner | T: +1.512.721.2721
He | Him | His

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen <SteveRoth@eversheds-sutherland.us>
Sent: Friday, September 4, 2026 10:31 AM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; mjwilson-bilik@eversheds-sutherland.com
Subject: Summary and Analysis of NAIC Full Draft of Revised Model 672; CAI Call Wednesday 9/9 @ 2pm ET

Hello everyone,

We are scheduling a call of the CAI's Cyber & Privacy Working Group next **Wednesday, September 9 at 2 pm ET** to discuss the full draft of revised Model #672 that the NAIC's PPWG exposed for comment several weeks ago (Full Revised Draft) and possible CAI comments on that draft. *We will be sending out a calendar meeting invitation for the call.*

Since the Full Revised Draft was released, we have been reviewing and analyzing it in some detail in order to assist this CAI Working Group in identifying those specific issues and concerns that merit CAI comment. Comments are due September 22. To that end, we have prepared and are attaching for your information and review:

- A memo that summarizes the key provisions in each Article of the Full Revised Draft, focusing on the notable changes that have been made (or not made) to the version of each Article that the PPWG previously exposed for comment. The memo includes our analysis/commentary on those provisions of each Article that we believe are particularly concerning. The memo also references to those changes that the PPWG has made that are responsive to comments the CAI previously submitted.

EVERSHEDS SUTHERLAND

- The Revised Full Draft that the PPWG released (which shows the PPWG's proposed changes to current #672) that now includes margin notes we have added comment ing on particular provisions and possible comments that could be made on those provisions.

We hope you find these materials to be helpful and informative. We plan to use next Wednesday's call to give everyone an opportunity to provide input on the form and content of the CAI's comments. Given the number and breadth of the issues raised by the Full Revised Draft , we don't expect we will be able to discuss every issue on next Wednesday's call, but we hope we can come away with a consensus on the key issues and how to address them. If necessary, we will schedule a follow up call to provide an opportunity for full discussion. To the extent you are able to review the attachments before the call, that of course will be helpful.

Please feel free to reach out to Al Sand (512-721-2721), Mary Jane Wilson-Bilik or me with questions or comments prior to the call. In the meantime, we hope you have an enjoyable Labor Day holiday week-end!

Regards,

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

---

From: Roth, Stephen <SteveRoth@eversheds-sutherland.us>
Sent: Monday, July 27, 2026 6:17 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: NAIC Exposure of Full Draft of Revised Model 672

Dear CAI Cyber & Privacy Working Group Members,

We are writing to update you on the NAIC Privacy Protections (H) Working Group's (PPWG) ongoing work to revise Model 672. **On Friday 7/24, the PPWG exposed a full draft of revised Model 672 for public comment, with comments due by September 22, 2026.** Please see the attached.

This full draft brings together all the segments of Model 672 previously exposed and revised by the PPWG along with a newly revised definitions section, which includes proposed definitions for key terms such as "sale" and "targeted advertising" among others. The PPWG will hear initial oral comments on the full revised draft during its meeting at the NAIC Summer National Meeting on Aug. 13, 2026, but we expect comments at the meeting will be fairly limited given the short amount of time available to stakeholders to analyze the draft.

We are reviewing and working through the draft and will follow up to provide our initial analysis of the complete draft and key issues.

In the meantime, if you have any questions, please contact Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) or me.

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

EVERSHEDS SUTHERLAND

From: Roth, Stephen
Sent: Thursday, June 4, 2026 5:37 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: Update on NAIC PPWG's Work on Revising Model 672

Dear CAI Cyber & Privacy Working Group Members,

We are writing to update you on the NAIC Privacy Protections (H) Working Group's (PPWG) ongoing work to revise Model 672. ***The PPWG is now in the process of putting together the fully reconstructed Model, which it plans to expose for public comment ahead of the Summer National Meeting (August 11-14).*** The PPWG will hold a one-hour public meeting at the Summer National Meeting to hear comments on the revised Model. As you know, the PPWG did not include the definitions of key terms (e.g., "sale" and "targeted advertising") with the individual sections that were previously released, which significantly limited the CAI's and other interested parties' ability to assess the scope and potential impact of the revised Model and provide meaningful comments. We expect the CAI will have extensive comments when the fully reconstructed Model is released.

On June 3, the PPWG held a meeting to discuss comments on the proposed revisions to Article VIII of Model 672 (Additional Provisions). A copy of the Committee's May 6 final comment letter conveying the Committee's support for new Section 31, which provides that violations of the Act do not give rise to a private right of action, is attached for your reference.

During the meeting, consumer advocates urged the PPWG to add language to Section 31 indicating that nothing in the Act should be construed to invalidate a pre-existing private right of action. Chair Dwyer expressed her general support for adding language to preserve any pre-existing private right of action but recommended that the exact wording should mirror a similar provision in the NAIC's Insurance Data Security Model 668 (the text of which is copied below) to promote consistency across NAIC Models. Dan Bumpus (VA) and Mark Fowler (AL) indicated their support for the proposed language.

"This Act may not be construed to create or imply a private cause of action for violation of its provisions *nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.*" (emphasis added)

Additionally, consumer advocates suggested that a drafting note could be added to clarify that Section 31 is optional and states may choose to provide for a private right of action. Chair Dwyer disagreed with this approach, noting that states are not obligated to adopt an NAIC model as drafted and the proposed language was thoroughly vetted under Model 668 to address both industry and consumer advocates' concerns.

We will continue to monitor and report on any developments as the PPWG assembles the full revised Model. In the meantime, if you have any questions please contact Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) or me.

Regards,

Steve

Stephen E. Roth | Partner | T: +1.202.383.0158

EVERSHEDS SUTHERLAND

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen
Sent: Wednesday, April 8, 2026 5:54 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: NAIC PPWG Requests Comments on Revisions to Article VIII of Model 672

Dear Cyber & Privacy Working Group Members,

We are writing to update you on the NAIC Privacy Protections (H) Working Group's (PPWG) ongoing work to revise Model 672. On April 6, 2026, the PPWG issued a call for comments on the revisions to Article VIII of Model 672 (Additional Provisions) for public comment (*attached*). **Comments on Article VIII are due on May 6, 2026.**

Revised Article VIII. Article VIII covers a number of miscellaneous provisions, including (i) the supremacy of the federal Fair Credit Reporting Act over the Model; (ii) nondiscrimination against consumers who choose to opt-out of disclosure of their nonpublic personal financial information or who choose not to grant authorization for the disclosure of their nonpublic personal health information; and (iii) how violations of the Model should be addressed. Revised Article VIII is largely unchanged from the corresponding section of current Model 672. *In a welcome change, however, new Section 31 (Individual Remedies) has been added to establish that violations of the Model do not give rise to a private right of action.*

Proposed CAI Comment Letter on Article VIII. Although we ultimately determined following our last call of the CAI's Cyber & Privacy Working Group not to comment on the PPWG's February exposure of proposed revisions to Article VII of Model 672, we do believe it would be worthwhile to comment on this exposure of revised Article VIII. Specifically, we recommend that the Committee submit a short comment letter in support of new Section 31 to counterbalance any comments arguing in favor of a private right of action that may be submitted***. Please let us know if you have concerns with this approach or if there are any additional comments on revised Article VIII that we should include.*** We will plan to circulate a draft of the CAI comment letter for your review next week, and then to submit the final comment letter by the May 6 deadline.

Next PPWG Steps. After Article VIII, the sole article that remains to be exposed for public comment is Article I, which includes the definitions of key terms (e.g., "sale" and "targeted advertising") that will be essential to determining the scope and potential impact of the revised Model as a whole. The PPWG has not provided a timeline of when revisions to Article I will be released, but it is expected in the coming months.

In the meantime, if you have any questions please reach out to Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660), or me.

Regards,

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

EVERSHEDS SUTHERLAND

From: Roth, Stephen
Sent: Tuesday, February 10, 2026 11:38 AM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: PPWG Revisions to Article VII and New Revisions to Article VI of Model 672 - CAI Call Scheduled Tuesday February 17 @ 4 PM ET

Dear Cyber & Privacy Working Group Members,

We are writing to update you on the NAIC Privacy Protections (H) Working Group's (PPWG) ongoing work to revise Model 672, including revisions to Article VII (*Rules for Health Information*) and new revisions to Article VI (*Exceptions to Limits on Disclosures of Nonpublic Personal Information*). As you know, the Committee of Annuity Insurers had previously commented on the PPWG exposure of the draft revised Article VI. Set forth below is a summary of these most recent developments along with our commentary regarding continuing areas of concern.

Revised Article VII
Yesterday, the PPWG issued a call for comments on the revisions to Article VII of Model 672 (*Rules for Health Information*) (attached). *Comments on Article VII are due on March 11, 2026*.

Article VII covers when an individual's nonpublic personal health information may be disclosed, what constitutes a valid authorization of such disclosure, how requests for authorization may be conveyed, and the relationship between the Model's requirements and other applicable federal and state laws and regulations. Revised Article VII is largely unchanged from the corresponding section of current Model 672. However, Section 25 (*Relationship to Federal Rules*) has been revised to reflect that compliance with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will *not* exempt a licensee from the requirements of Article VII unless the licensee is actually subject to HIPAA. Previously, the exemption from Article VII extended to any licensee that complied with the requirements of HIPAA, even if they were not otherwise required to do so. This change means that if HIPAA does not apply to an insurer, the insurer must either obtain a valid authorization or rely on another exception for specified insurance functions provided in Article VII to disclose nonpublic personal health information. Those exceptions remain the same as under current Model 672.

Revised Article VI
Yesterday, the PPWG also released a revised version of Article VI of Model 672 (*Exceptions to Limits on Disclosures of Nonpublic Personal Information*) based on comments received during the previous comment period. We have attached clean and redline copies of the February 9 version of Article VI as well as the Committee's October 10 comment letter on the previous version for your reference. *The PPWG is **not** seeking additional comments on Article VI at this time.*

Article VI covers exceptions to the limits on disclosure of Nonpublic Personal Information (NPI), including exceptions for service providers and joint marketing, processing and servicing transactions, and other specified business and legal purposes (*e.g.*, in connection with a merger or similar business transaction, in response to law enforcement, to comply with legal and regulatory requirements, etc.). Article VI is substantially unchanged from the version previously exposed for comment. It continues to provide for a new exception to notice and opt-out requirements for responding to security incidents and, unfortunately, it continues to provide no exceptions to the opt-in requirements for the sale of NPI and the disclosure of sensitive personal information (SPI).

EVERSHEDS SUTHERLAND

Importantly, although the joint marketing exception has been retained in revised Article VI, a drafting note indicates that for purposes of this revised draft, the PPWG decided not to address comments recommending that the joint marketing exception should be removed. However, if the comments are raised again after the full exposure of the revised Model, the PPWG will address them at that time. As reflected in the November 7, 2025 public discussion of comments on Article VI we previously reported on, the joint marketing exemption and opt-out vs. consent will continue to be a central issue going forward.

We are scheduling a CAI Working Group call on **Tuesday, February 17 from 4-4:45 pm ET** to discuss feedback from Committee members on revised Article VI and potential comments that the Committee should submit. We will be sending out a Zoom invitation for the call.

In the meantime, if you have any thoughts or questions about the PPWG's most recent release of revised Articles VI and VII, or if you can't join the call and would like to share your thoughts about issues and concerns the Committee should address, please reach out to Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660), or me.

Regards,

Steve

Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen
Sent: Wednesday, November 12, 2025 12:37 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: Update on PPWG's Work on Revising Model 672: New Revisions to Article V and Discussion of Comments on Draft Revisions to Article VI

Dear Cyber & Privacy Working Group Members,

We are writing to update you on the NAIC Privacy Protections (H) Working Group's (PPWG) ongoing work to revise Model 672, including new revisions to Article V (*Limits on Disclosures of Nonpublic Personal Information*) and PPWG discussion of comments on draft revisions to Article VI (*Exceptions to Limits on Disclosures of Nonpublic Personal Information*). As you know, the Committee of Annuity Insurers had commented on the PPWG exposures of both draft revised Articles V and VI. Set forth below is a summary of these most recent developments along with our commentary regarding continuing areas of concern.

Revised Article V
On November 7, 2025, the PPWG released a revised version of Article V of Model 672 (*Limits on Disclosures of Nonpublic Personal Information*) based on comments received during the previous comment period. Article V has been significantly revised from the version previously exposed for comment in May. We have attached clean and redline copies of the November 7 version of Article V as well as the Committee's June 18 comment letter on the previous version for your reference. *The PPWG is **not** seeking additional comments on Article V at this time.*

Article V focuses on limits on the disclosure of NPI, including provisions providing an affirmative *opt-in* (consent) requirement prior to the sale of NPI or disclosure of Sensitive Personal

Information (SPI), and *opt-out* rights from disclosure of NPI for targeted advertising. The terms "targeted advertising" and "sale" remain undefined. The definitions of these terms will be essential to determining the scope and potential impact of the Article V opt-out and opt-in requirements. Article V also contains edits to streamline the revised language (e.g., cross-referencing to the notice requirements detailed in other sections rather than specifying details to be included in such notice).

Section 18 – General Rules for Use and Disclosure of NPI
A new subsection has been added to Section 18 which provides that, in general, a licensee may use or disclose NPI: (i) to process a "business transaction" entered into by the licensee and consumer, (ii) to an affiliate if the affiliate's use and disclosure of NPI complies with the Act, and (iii) to nonaffiliated third parties only in compliance with the Act. It also specifies that if an opt-out request is received during the course of a transaction that would conflict with the processing of that transaction, the licensee must notify the consumer of this conflict and confirm the consumer's authorization to continue the transaction. This could be administratively difficult to apply, potentially requiring new functionality to detect these kinds of conflicts and obtain confirmation as part of the transaction workflow. It is also unclear how this provision would interact with the Article VI exceptions, including for processing and servicing transactions, potentially limiting the ability of companies to rely on those exemptions without engaging the consumer.

In a concerning change from the previous version, the exception to the general limit on the disclosure of NPI to a nonaffiliated third party before the consumer has been provided with notice and the opportunity to exercise opt-out or opt-in rights is no longer "as otherwise authorized in this Act" — rather, the *only* specified exception is where the licensee is processing a business transaction entered into by the licensee and consumer. This would significantly restrict the ways in which information may be shared prior to providing notice, and may be untenable in some circumstances, as it excludes critical Article VI exceptions for joint marketing, law enforcement, fraud detection, and cybersecurity investigations, among others.

In addition, Section 18 now provides that the consumer should be given a reasonable opportunity to opt-out of the "transaction" before NPI is disclosed to a nonaffiliated third party, rather than the "disclosure," suggesting that consumers would need to have the ability to cancel an existing transaction once informed that NPI would be disclosed to non-affiliated third parties as part of that transaction. This appears to conflict with the exemption from the notice requirement for disclosing NPI for purposes of processing a business transaction, and may be a drafting error. Further, the insurer must "receive and document" the consumer's election to opt-in or opt-out, as applicable, before disclosing NPI to a nonaffiliated third party. We note that an insurer would not "receive" anything if a consumer does not elect to exercise opt-out rights and therefore the insurer should not be required to "receive" the consumer's election prior to disclosure where there is an opt-out right. Finally, the definitions for "opt-out" and "opt-in" and their respective provisions for what constitutes a reasonable opportunity to opt-out or opt-in have been deleted from Section 18. Presumably, these definitions should appear in the revised Definitions section when it is released for public comment.

Section 19 – Limits on Re-Disclosure and Reuse of NPI
In a welcome change, the Article VI exceptions have been incorporated into Section 19 as the CAI recommended. However, this section continues to apply only to NPI a licensee receives from or shares with a nonaffiliated third party service provider, despite the CAI's recommendation that it should also apply to NPI received from or shared with nonaffiliated financial institutions who are not service providers (e.g., NPI disclosed from a ceding insurer to a reinsurer). It would seem that non-service providers would fall under the general rules articulated in Section 18, discussed above.

Further, a number of expressly permitted re-disclosures of NPI in Section 19 have been stripped out. Section 19 no longer generally allows re-disclosure of NPI in ways the original disclosing

party would have been permitted to disclose the NPI directly. Re-disclosure of NPI is now permitted only as follows:

- NPI received from a nonaffiliated third party service provider under an exception may only be disclosed to carry out the activity covered by that exception – *not* to affiliates of the third party service provider from which it was received or to the licensee's own affiliates;
- NPI received from a nonaffiliated third party service provider *other than* under an exception may be disclosed to affiliates of the third party service provider from which it was received or to the licensee's own affiliates – *not* to any other person;
- NPI disclosed to a nonaffiliated third party service provider under an exception may only be disclosed to carry out the activity covered by that exception or to the licensee's affiliates – *not* to affiliates of the third party service provider; and
- NPI disclosed to a nonaffiliated third party service provider *other than* under an exception may be disclosed to the licensee's affiliates (who may disclose the NPI only to the extent permissible for the licensee) and to any other person, if the disclosure would be lawful if made directly to that person by the licensee – *not* to affiliates of the third party service provider if disclosure would not otherwise be lawful under the Act.

Section 21 – Limits on Disclosure of NPI in Targeted Advertising
As with the previously proposed revisions to Article V, the most recent version requires that consumers be given the opportunity to opt-out of the disclosure for NPI to a nonaffiliated third party for targeted marketing purposes. The 15-day timeline for acting on a consumer's opt-out request was not extended to 30 days as recommended by the CAI. It continues to conflict with the 10-day timeline in a parallel requirement as part of revised Article IV.

In addition, previously proposed language describing how a licensee may satisfy the opt-out requirement by providing a cookie banner or link on the footer of their website homepage or by providing another method that can effectively identify a person and remove them from targeted advertising has been removed and a new provision clarifies that the consumer has the right to opt-out of targeted advertising at any time.

Section 22 – Limits on Sale of NPI
Revised Article V retained the requirement for licensees to obtain consumer opt-in (consent) prior to the sale of NPI. What constitutes a "sale" remains undefined but will presumably be addressed once a definitions section is exposed for comment.

Section 23 – Limits on Disclosure of SPI
Revised Article V continues to require consumer opt-in (consent) to disclose SPI other than under an Article VI exception. Section 23 continues to apply to all disclosure of SPI, not just to the disclosure of SPI to nonaffiliated third parties which the CAI had recommended. This deviates from other limitations on disclosure that clearly specify that disclosure of NPI to nonaffiliated third parties is what is restricted (e.g., Section 21 on targeted advertising and the general opt-out right under Section 18). However, we note that Section 23 permits disclosure of SPI without the consumer's affirmative opt-in consent "for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of the Act." This would appear to include the new subsection of Section 18 that, as noted above, allows the disclosure of NPI to affiliates if the affiliates' use and disclosure of NPI complies with the Model.

Public Discussion of Comments on Article VI
On November 7, the PPWG held a meeting to discuss comments on proposed revisions to Article VI of Model 672, which covers exceptions to the limits on disclosure of Nonpublic Personal Information (NPI), including exceptions for service providers and joint marketing, processing and servicing transactions, and other specified business and legal purposes. During the meeting, Damon Diedrich (CA) raised concerns about the joint marketing exception, arguing that consumers should have the ability to opt out of joint marketing. Industry representatives underscored the importance of joint marketing to the industry and cautioned against changes

EVERSHEDS SUTHERLAND

that could disadvantage insurers from other financial services, making it harder to compete in the broader market. Bob Wake (ME) expressed skepticism that joint marketing provides enough benefit to consumers to justify the exception over a consumer's objections.

Moving forward, the PPWG does not have a firm timeline for releasing additional sections of the Model for public comment. At the National Meeting in December, the PPWG intends to request an extension of time to Fall 2026 to finalize the revisions to Model 672.

We will continue to monitor and report on any developments as the PPWG continues to revise Model 672. In the meantime, if you have any questions please contact Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660), or me.

Regards,

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen
Sent: Tuesday, October 21, 2025 6:14 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: Final CAI Comment Letter on Revised Article VI of Model 672 Chair's Draft

Dear CAI Cyber & Privacy Working Group Members,

Attached for your reference is the final CAI comment letter on revised Article VI of NAIC Model Law 672, which was submitted to the NAIC Privacy Protections (H) Working Group (PPWG) for consideration. The feedback we received was supportive of the draft comments we circulated on October 3. Accordingly, the final comment letter recommends that the Article VI exceptions apply to the proposed opt-in requirements, supports the additional exemption for information sharing around security incidents, and reaffirms the Committee's previous comment that the Section 26 exceptions should apply to all nonpublic personal information (not just nonpublic personal financial information as currently drafted).

We will continue to report any developments as the PPWG continues its work on the revised Model. In the meantime, if you have any questions please contact Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) or me.

Regards,

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen
Sent: Friday, October 3, 2025 5:00 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>

EVERSHEDS SUTHERLAND

Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: Draft CAI Comment Letter on Revised Article VI of Model 672 Chair's Draft - Comments Requested

Hi everyone,

Following up on our September 29 note below, we are providing you with a draft of the CAI's comment letter on revised Article VI of NAIC Model Law 672.

The attached draft comments that the Article VI exceptions should apply to the proposed opt-in requirements as noted in our e-mail below, reaffirms the Committee's September 18, 2024 comment on the Chair's Draft (attached) that the Section 26 exceptions should apply to all nonpublic personal information (not just nonpublic personal financial information as currently drafted), and suggests corresponding revisions to the language of Article VI.

Because comments are due on Friday, October 10, *we ask that you provide us with any comments or edits to the attached draft by* ***next Wednesday, October 8 at 6 pm ET*****.** Please send any comments you have to Al Sand (512-721-2721) , Mary Jane Wilson-Bilik (202-383-0660), or me.

Have a nice week-end!

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen
Sent: Monday, September 29, 2025 6:03 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: PPWG Exposes for Comment Revised Article VI of Model 672 Chair's Draft; CAI Member Input Sought on CAI Comment Letter

Dear CAI Cyber & Privacy Working Group Members,

We are writing to update you on the NAIC Privacy Protections (H) Working Group's (PPWG) ongoing efforts to develop an updated NAIC privacy model law based on the Chair's Draft revisions to existing NAIC Model Law 672.

Revised Article VI. On September 26, 2025, the PPWG issued a call for comments on the revisions to Article VI of the Model (attached). **Comments on Article VI are due on October 10, 2025.**

Article VI covers exceptions to the limits on disclosure of Nonpublic Personal Information (NPI), including exceptions for service providers and joint marketing, processing and servicing transactions, and other specified business and legal purposes (*e.g.*, in connection with a merger or similar business transaction, in response to law enforcement, to comply with legal and regulatory requirements, etc.). Revised Article VI does not contain any substantive changes from the previously proposed Chair's Draft and largely mirrors the language of Article IV of existing Model 672. As was reflected in the Chair's Draft, revised Article VI upon which the PPWG now is seeking comments includes a new exception to notice and opt-out requirements when a licensee

EVERSHEDS SUTHERLAND

discloses nonpublic personal financial information to "prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information."

Importantly, we note that *Article VI has **not** been revised to provide exceptions to **opt-in** requirements of any kind*. This omission is critical in light of revised Article V (attached, together with a copy of the Committee's June 18, 2025 comment letter thereto). As currently drafted, the Article VI exceptions would not apply to the requirement for a consumer to opt-in before a licensee may "sell" (a term which remains undefined) NPI under Section 22 of revised Article V. If the "sale" of NPI is defined broadly, it could potentially include reinsurance transactions, mergers and acquisitions, and other significant business transactions for which the Article VI exceptions are crucial. Moreover, Section 23 of revised Article V provides that a licensee may disclose a consumer's sensitive personal information (SPI) *only as expressly permitted or required by Article VI or other provisions of the Act* unless the consumer has opted in. In the absence of exceptions for opt-in requirements in revised Article VI (which would appear to be the Working Group's intent), the disclosure of SPI would be completely prohibited without opt-in consent (unless some other provision of the Model allowed it).

Proposed CAI Comment Letter. As part of our ongoing work on these issues, we plan to submit a comment letter on behalf of the Committee and therefore we are seeking feedback from Committee members on those issues and concerns raised by revised Article VI that Committee members believe we should comment upon. We anticipate that our comment letter would emphasize the importance of applying Article VI exemptions to the new opt-in requirements proposed under the most recent revisions of the Chair's Draft and propose red-line language for doing so. We would be supportive of the additional exemption for information sharing around security incidents.

Please let us know at your earliest convenience if you have concerns with or comments on this proposed approach. Please also let us know if there are any additional exemptions that we should propose be added to Article VI.

We will plan to circulate a draft of the CAI comment letter for your review by the end of this week, and then to submit the final comment letter by the October 10 deadline.

In the meantime, if you have any questions please contact Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) or me.

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen
Sent: Thursday, June 19, 2025 5:31 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: CAI Comment Letter on NAIC PPWG Exposure of Revised Article V of Model 672 Chair's Draft

Hi everyone,

EVERSHEDS SUTHERLAND

Yesterday we submitted the Committee of Annuity Insurer's comment letter on revised Article V of the Model 672 Chair's Draft to the NAIC PPWG. It is attached for your information and reference.

We really appreciate all the helpful input, direction and comments from members of the CAI's Cyber & Privacy Working Group on this latest missive from the PPWG. Thanks!

We will of course continue to monitor and report to you regarding further developments relating to revisions to Model 672.

Best,

Steve

Stephen E. Roth | Partner | T: +1.202.383.0158
From: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
Sent: Monday, June 16, 2025 4:37 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Mary Jane Wilson-Bilik (mjwilson-bilik@eversheds-sutherland.com) <mjwilson-bilik@eversheds-sutherland.com>; Roth, Stephen <SteveRoth@eversheds-sutherland.us>
Subject: RE: NAIC PPWG Exposure of Revised Article V of Model 672 Chair's Draft - Proposed CAI Comments

CAI Cyber & Privacy Working Group Members:

Following up on the below, attached is our draft comment letter on the NAIC PPWG's proposed revisions to Article V of the #672 Chair's Draft. Also attached for reference is the current proposed revisions to Article V.

Please provide any feedback by Noon ET on Wednesday June 18, so a final letter may be submitted by the EOD June 18 comment deadline.

If you have any questions, comments, or further thoughts, you can reach out to myself (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660), or Steve Roth (202-383-0158) (both copied above).

Best,

Al Sand

Alexander F. L. Sand | Partner | T: +1.512.721.2721
He | Him | His

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen <SteveRoth@eversheds-sutherland.us>
Sent: Thursday, June 12, 2025 5:11 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Mary Jane Wilson-Bilik (mjwilson-bilik@eversheds-sutherland.com) <mjwilson-bilik@eversheds-sutherland.com>

EVERSHEDS SUTHERLAND

Subject: NAIC PPWG Exposure of Revised Article V of Model 672 Chair's Draft - Proposed CAI Comments

CAI Cyber & Working Group Members:

Thank you to those who were able provide feedback on the NAIC PPWG's proposed revisions to Article V of the #672 Chair's Draft following our call last Friday. Based on that feedback, as well as coordinating conversations with the ACLI and other industry groups, we are working to draft a Committee of Annuity Insurers comment letter for submission by the June 18th deadline.

We plan to circulate a draft by Monday, June 16, and will ask for any feedback by Noon ET on Wednesday June 18, so a final letter may be submitted by the EOD June 18 comment deadline.

We are currently planning to focus the Committee's comments on the following issues:

· The Committee's ability to meaningfully comment on the proposed language, and proposed revisions to Model 672 generally, is significantly limited by the piecemeal approach of releasing proposed language. Here, evaluating the impact of proposed revisions to Article V is necessarily dependent on exceptions provided in Article VI and the meaning of the undefined key terms "sale" and "targeted marketing". Overly broad definitions of these terms or future revisions to Article VI would substantively alter the meaning and impact of the current proposed revisions to Article V. Accordingly, it is imperative that at some point the PPWG expose a comprehensive proposed draft of Model 672 that would allow stakeholders to more meaningfully assess and comment on the proposed revisions. It is important that current Article VI exemptions, which were thoughtfully crafted and time-tested, remain.

· The Committee appreciates that the proposed revisions to Article V recognize that an opt-out approach is appropriate in many circumstances to provide meaningful privacy protections to consumers without unduly impeding the ability of insurance licensees to conduct normal operations and compete in the broader financial services marketplace. However, the opt-in (consent) approach for limiting the sale of NPI or disclosure of SPI would pose meaningful challenges and would put the insurance industry at a competitive disadvantage with other financial services providers. That said, we recognize and appreciate the Working Group's efforts to find a workable compromise between the contrary approaches being advocated for by different groups of stakeholders.

· As noted, the Committee continues to be concerned about an opt-in approach, including a limited opt-in approach, because it will put annuity insurers at a competitive disadvantage compared to competing non-insurance retirement products. Those competing products are regulated under GLBA through the SEC's recently updated Regulation S-P, which continues to take an opt-out approach consistent with current Model 672. If annuity insurers are hamstrung from competing, the result is that consumers who would benefit from having access to annuity products are less likely to have such access.

· Suggest definition of a "sale" (CAI previously submitted the following definition when revised Article III was exposed):
o *"Sale" or "selling" of nonpublic personal information means the exchange of nonpublic personal information for monetary consideration by the licensee to a non-affiliated third party. "Sale" or "selling" nonpublic personal information does not include:*
(1) The disclosure of nonpublic personal information to a service provider that processes the nonpublic personal information on behalf of the licensee;
(2) The disclosure of nonpublic personal information to a third party for purposes of providing a product or service requested by the consumer or as otherwise permitted under Article VI of this Act;
(3) The disclosure or transfer of nonpublic personal information to an affiliate of the licensee;

EVERSHEDS SUTHERLAND

(4) The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or (5) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the licensee's assets.

· Suggest definition of "targeted marketing". While the CAI has not previously provided a suggested definition, the industry draft submitted by a joint trade group included the following:
o *(1) "Targeted advertising" means displaying online advertisements to a consumer where the advertisement is selected based upon data that is linked or reasonably linkable to an identified or identifiable natural person obtained from that consumer's activities across nonaffiliated websites or online applications over time to predict such consumer's preferences or interests.*
o *(2) "Targeted advertising" does not include:*
§ *(a) Online advertisements based on activities within a Licensee's own websites or online applications;*
§ *(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;*
§ *(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or*
§ *(d) Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.*

· Clarify that limits on disclosure of SPI apply to disclosures to nonaffiliated third parties. This is not clear as drafted, and could be read to limit disclosure to affiliates.

· Fix conflicting timelines to comply with opt-out requests (15-days vs. 10 days).

· Clarify the definition of opt-in as a knowing and "intelligent" agreement. Unclear what "intelligent" would mean. Revise as "knowing and intentional" or just "knowing.

Please let us know if you have any questions, comments or further thoughts based on the above*. *You can reach out to Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) (both copied above) or me.

Regards,

Steve
Stephen E. Roth | Partner

steveroth@eversheds-sutherland.com
T: +1.202.383.0158
Biography

Eversheds Sutherland
Helping our clients, our people and our communities to thrive
From: Roth, Stephen
Sent: Tuesday, June 3, 2025 4:36 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: NAIC PPWG Release of Revised Articles IV & V of Chair's Draft - CAI Call Friday June 6 @ 2 pm ET

Dear CAI Cyber & Privacy Working Group Members,

EVERSHEDS SUTHERLAND

We are writing to summarize the May 19th release by the NAIC Privacy Protections (H) Working Group (PPWG) of revised Articles IV and V of the Chair's Draft of revised Model Law 672 (both attached), and to schedule a call of the CAI's Working Group to discuss those issues and concerns that a Committee of Annuity Insurers comment letter should address.

Article V focuses on limits on the disclosure of Nonpublic Personal Information (NPI). **Comments on revised Article V as exposed are due June 18, 2025**.

Revised Article V of the Chair's Draft now includes language that was previously exposed by the PPWG as part of its revisions to Article III, and was tagged at that time as language that would ultimately be moved to Article V. Moving this language to Article V from Article III is consistent with the Committee's previous comments on Article III. Specifically, this includes previously released (but not exposed for comment) language establishing:

- Consumer opt-out rights from the disclosure of NPI for targeted advertising;
- An affirmative opt-in requirement for the sale of NPI; and
- An affirmative opt-in requirement prior to the disclosure of Sensitive Personal Information (SPI).

The terms "targeted advertising" and "sale" remain undefined. The definitions of these terms will be essential to determining the scope and potential impact of these opt-out and opt-in requirements. For any disclosure of NPI to a third party that does not fall under one of these categories (i.e. targeted advertising, sale, or disclosure of SPI), the existing opt-out requirements of Model 672 would apply.

The PPWG also released a revised version of Article IV (privacy notice requirements) based on comments received during the previous comment period. Revised Article IV deviates substantially from the version previously exposed for comment. Because that version was generally consistent with existing notice requirements under Model 672, the Committee did not submit a comment letter. **However, revised Article IV is not being exposed for additional comment at this time**.

A more detailed summary of the changes to both Articles IV and V is provided in the attached memo that we have prepared for your information and review.

As part of our ongoing work on these issues, we anticipate submitting a comment letter on behalf of the Committee on issues of concern to Committee members that are raised by Article V. ***We are scheduling a CAI Working Group call this Friday, June 6 at 2pm ET to discuss feedback from Committee members and potential comments that the Committee should submit on revised Article V.*** The details for that call are as follows:

DATE AND TIME: Friday, June 6 @ 2-3pm ET

Join By Telephone	
Dial In:	+1 646 558 8656
Meeting ID:	5787221869
Pass Code:	339516
Join Web-Based Meeting	**Zoom Link**
One-Tap Mobile:	+16465588656,,5787221869#,,,,*339516#
Meeting URL:	https://eversheds-sutherland-us.zoom.us/j/5787221869?pwd=K1FoZTRweG0ybFVoUnZCVHd1WUczdz09

EVERSHEDS SUTHERLAND

We will also send a calendar invite to Working Group members for the call. In the meantime, if you have thoughts or questions about the PPWG's most recent release of revised Articles IV and V, and/or can't join this Friday's call and would like to share your thoughts about the issues and concerns that the Committee's comment letter should address, please reach out to Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) or me.

Regards,

Steve
Stephen E. Roth | Partner | T: +1.202.383.0158

Eversheds Sutherland
Helping our clients, our people and our communities to thrive

From: Roth, Stephen
Sent: Tuesday, March 11, 2025 12:29 PM
To: CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
Cc: Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>
Subject: Update on PPWG's Work to Update NAIC Model Law #672

Hello everyone,

We are writing to provide an update on the progress of the NAIC's Privacy Protections Working Group (PPWG) to update Model Law # 672.

Revisions to Article III of the Chair's Draft

On February 25, the PPWG released new revisions to Article III of the previously proposed Chair's Draft, following a comment period during which we had submitted a comment letter on behalf of the Committee (attached). Article III contains many of the same substantive changes included in the Chair's Draft, including new consumer rights to access, correction, and deletion , limits on the sale of nonpublic personal information (NPI), and limits on the use and disclosure of sensitive personal information (SPI).

Revised Article III (also attached) makes a number of substantial revisions to the previous version, including some changes reflecting our recommendations, but retains a number of concepts about which we expressed concerns. Several provisions from the Chair's Draft have also been relocated, renamed, or replaced. Additionally, there are entire new sections which are called out as applicable. A summary of the key revisions is set forth below for your information.

Section 6 – Access, Correction, and Deletion of Nonpublic Personal Information

- Section 6 has been revised in several places to clarify that requests must be "authenticated," replacing previously inconsistent and unclear requirements to "verify" or "authorize" consumer requests. This change is consistent with our submitted comments.

Section 6(a) – Access Right

- Revised section 6(a) no longer includes language requiring the response to be made in a consumer defined format. This change is consistent with our comments.
- Section 6(a) revisions also include edits clarifying existing exemptions for responding to duplicative requests and new language stating that the licensee is not obligated to

provide information beyond the scope of the request if the consumer has specified particular items.
- Section 6(a) has retained the requirement for licensees to provide consumers with the list of all third-party service providers to which the licensee disclosed the consumer's nonpublic personal information. This is in contrast to our submitted comments, which highlighted the challenge and burden of maintaining and providing this information while providing little value to consumers.

Section 6(b) – Correction Right

Revised Section 6(b) includes the following changes:

- A response to the consumer is now required within 45 days of a request to correct information, revised up from 30 days. Note that there is currently already an obligation to respond to correction requests within 30 days under Model 670.
- Licensees now have the option to delete information, in addition to correcting or denying the correction, upon receiving a request to correct.
- Addition of the ability for consumers to appeal if the licensee denies their request to change information, and a licensee is required to provide information about the appeals review process and notify the consumer of the decision.
- New language regarding the denial of a request to correct information when the licensee is not the creator of the information. The licensee may deny the correction unless the originator is no longer available to amend the information, and the consumer can independently demonstrate that the provided information is correct.

Section 6(c) – Deletion Right

- Revised Section 6(c) now allows licensees to delay deletion of data stored on archive or backup systems by 45 days, increased from 30 days. This revision is inconsistent with our comment, which requested that data not be required to be deleted until that system is next accessed in the ordinary course.
- In contrast to our comment and suggested revisions for a more comprehensive list of exemptions, revised Section 6(c) maintains the same short list of exemptions from the right to deletion as defined in the Chair's Draft.

Section 6(d) – Request and Response Requirements

Revised Section 6(d) provides more detailed guidance on the expectations for authenticating and responding to consumer rights requests. These changes include:

- New language requiring that licensees use commercially reasonable methods to authenticate the identity of requesters and allowing requests to be submitted by third-party agents/representatives, parents, or guardians.
- Allowing licensees not to respond to a request if the personal information at issue "is not locatable or retrievable by the licensee." This revised language removes the previous "impossible" standard consistent with our comment letter, but does not adopt the "disproportionate effort" standard we suggested. A new drafting note also directs examiners to review a licensee's justification for where it determines personal information is not locatable or retrievable.
- A new requirement to notify consumers if the licensee is unable to fulfill the request.
- A requirement that in the event a consumer disagrees with a licensee's refusal to correct NPI, the consumer may file a statement with the licensee stating why they disagree with the licensee's decision as well as what the consumer thinks is accurate information.
- The previously included cap on the number of requests to correct or delete information in a 12-month period has been removed.

EVERSHEDS SUTHERLAND

Section 7 – Sale of NPI and Use of SPI

The Article III revisions also have significantly restructured what was formerly Section 7 and 8 of the Chair's Draft covering the sale of NPI and limits on the use and disclosure of SPI. Much of the substance of these requirements has been significantly revised and will be moved to Article V (Limits on Disclosure of NPI). Revisions include:

- Clearly requiring opt-in consent for the sale of NPI or the disclosure of SPI beyond uses specifically permitted under existing Article VI (Exception to Limits on Disclosures of NPI). What constitutes a "sale" of NPI has not yet been defined.
- Section 7 within Article III now focuses on the requirements for obtaining consent where required, including that the required consent must be authenticated and obtained separately from any other consent.
- New language has also been added requiring licensees to provide a notice to consumers describing what NPI will be sold or SPI will be disclosed and for what purposes prior to obtaining consent.
- Language suggesting that consumers might also be able to limit a licensee's internal uses of SPI has been removed.

These changes do provide requested clarification on the proposed approach to limiting the sale of NPI and disclosure of SPI, although they adopt an opt-in consent approach instead of an opt-out approach.

New Limitations on Disclosing NPI for Targeted Marketing

The revisions also include an entirely new proposed section establishing an opt-out right for the disclosure of NPI for targeted marketing purposes. Under this new requirement licensees may not disclose NPI to a non-affiliated third party for purposes of targeted marketing unless the consumer has the right to opt out of the targeted advertising or as is otherwise authorized under Model 672. This new provision includes:

- Licensee must provide clear and conspicuous instructions on how to opt out
- Licensees must act on opt-out requests within 15 days of receipt
- Licensees do not need to honor an opt-out request that does not match the licensee's records
- Licensees are under no obligation to obtain additional data to execute an opt-out request
- Licensees may not solicit consumers to change their opt-out for twelve months
- A licensee may comply with the opt-out requirement by providing a cookie banner on their website or another method if such approach can effectively identify a person and remove them from targeted advertising.

February 28 Meeting of the PPWG

The PPWG held a meeting on February 28, 2025 to hear comments on proposed revisions to Article IV (Privacy and Opt Out Notices for NPI) of the Chair's Draft. The Committee did not submit a written comment on these proposed changes as they were generally minimal and non-substantive.

During the call, consumer advocates and regulators from CA and VA used the opportunity to press their preference for an opt-in approach to any limitations imposed under a final revised Model 672, noting that most consumers will simply go with the default position and that therefore an opt-in approach is required to protect consumer interests. However, CA did recognize that insurance support organizations should be allowed to sell data that helps support

the industry. Industry representatives generally supported an opt-out approach, and emphasized the importance of maintaining a level playing field between the insurance industry and other industries. Maine expressed equivocation on whether opt-in or opt-out was the more desirable approach, and noted that they continue to struggle to determine which approach they will favor. There was general agreement that disclosure should be permitted to third parties without consent where needed to comply with legal or operational obligations.

Various industry representatives also took the opportunity to urge the PPWG to modernize the default requirements for privacy notice delivery to allow for electronic notice by default and paper delivery upon request. CA indicated that they thought initial notice should be in paper by default, allowing for opt-in to electronic delivery consistent with the Uniform Electronic Transactions Act.

Regarding next steps, Chair Dwyer stated they were still determining what the PPWG's approach would be moving forward. She did confirm that a more fulsome revision of Model 672 will be released for comment at some point, but is unsure whether there will be additional smaller comment periods prior to that happening.

The Committee's Continued Engagement

We plan to continue to engage with the PPWG to press our concerns regarding the issues raised in our comment letters, including submitting additional comments, as further revisions to Model 672 are opened for comment. We will be convening this Working Group to solicit your thoughts, reactions and input with respect to our continued advocacy. In the meantime we will continue to monitor and update you regarding the PPWG's ongoing efforts. Please don't hesitate to reach out if you have any questions.

Regards,

Steve