HINSHAW

Alerts

Beyond Data Breach: Evaluating Coverage for Misuse of Information Claims

July 6, 2020
Insights for Insurers

New and comprehensive privacy and cyber regulations continue to proliferate across the globe. These are not your father's data breach notification laws. The scope of information included within these mandates has expanded significantly beyond the limited categories of personally identifiable information found in early notification laws to now include broad categories of information like browsing history, biometric information, geolocation information, and audio, visual, thermal, and olfactory information, depending on the specific law or regulation at issue.

In addition, these mandates typically are not limited to data breach and disclosure situations; they often apply to how covered entities treat protected information throughout its entire lifecycle, from collection or creation, through use, retention, security, until ultimate disposition. They may create disclosure obligations concerning the entity's information-related practices as well as actionable rights for affected individuals. Some laws require that companies create certain roles such as a data protection officer or a chief information security officer, and establish requirements concerning oversight by corporate boards. They also may mandate creation of specific internal and/or publicly-facing written policies and procedures. In addition to empowering enforcement by a state attorney general or other governmental or regulatory agency, these new laws and regulations sometimes provide a private right of action to affected individuals, pursuant to which they can seek statutory and/or actual damages.

Achieving and maintaining compliance with these complex and constantly evolving privacy and security obligations can create both budgetary and operational challenges for many entities. Mistakes and mishaps are inevitable, even for those entities that fully embrace their obligations in good faith. Incidents can arise when entities act negligently or recklessly, or if they intentionally elect not to comply with legal requirements. This backdrop is leading to a higher frequency of regulatory actions and private lawsuits against covered entities that are quite different from "typical" data breach claims. How any given cyber insurance policy will respond to claims arising out of these information misuse claims requires a thoughtful analysis of the precise facts giving rise to the claim, the terms of the policy at issue, and the applicable law.

Cyber insurance policies typically include coverage for claims arising out of violations of cyber and privacy laws and regulations, but the coverage provided can vary greatly from policy to policy. When considering whether any given claim falls within a policy's coverage, the following issues should be considered:

- Scope of Coverage
  - Is coverage limited to only security events or breach/disclosure incidents, or is coverage triggered by, for example, claims arising out of an actual, alleged, or suspected breach of statutes or regulations with respect to the confidentiality, access, control, and use of protected or confidential information?
  - Does the policy apply to claims arising out of an alleged violation of a privacy or cyber law anywhere in the world or is coverage limited to specific laws or geographic areas?
  - Does the policy limit coverage to only specified violations of certain laws? For example, a policy may provide coverage for violations of the General Data Protection Regulation or the California Consumer Privacy Act, but limit that coverage to violations of only certain parts of those laws such as their information security provisions.
- Scope of Covered Information
  - The policy may limit the scope of information for which coverage is provided. For example, the policy may contain a list of categories of information to which coverage applies, apply only to information specified in breach notification

laws, or it may more cover information that is the subject of any law or regulation related to information security or privacy.

- Equitable Relief
  - Does the claim arise out of a demand for equitable or injunctive relief?
  - Consider how the policy defines terms like “loss” or “damages.”
  - Does the policy expressly preclude coverage for costs to establish or improve privacy or security practices?
  - Are costs for audit, reporting, and compliance specifically excluded?
- Compensatory Damages
  - Does the policy limit coverage to “compensatory” damages? If so, statutory damages that do not require the calculation of any actual damages to the claimant may not be covered.
- Fines and Penalties
  - Does the policy expressly provide coverage for fines and penalties?
  - Consider the applicable law.
    - Does the policy contain a choice of law provision?
    - Is coverage for fines and penalties dependent on the law of a specific jurisdiction, such as the fining jurisdiction, the jurisdiction that most favors coverage, or the jurisdiction with a substantial relationship to the insured, the insurer, the policy, or the claim?
  - Is the fine or penalty at issue punitive in nature?
    - If so, does the applicable law preclude coverage, even if the liability is vicarious?
  - Does the claim arise out of intentional acts?
    - Does an intentional acts exclusion apply?
    - Is there an exclusion for knowing or willful violations of statutes?
    - Consider the application of imputation of knowledge provisions.
    - Does the applicable law prohibit coverage for intentional or non-fortuitous acts?

Conclusion

Cyber insurance policies typically provide broad coverages for a wide range of cyber and privacy risks, but that doesn’t mean that every claim involving the misuse of information will be covered under every policy. Insurers should closely review each claim at issue in light of the relevant policy language and applicable law.