"Cyber" Policies

- Cyber and privacy exposures are ever evolving and claims scenarios are often complex.
  - *E.g.*, Hollywood Presbyterian Hospital computers locked for over a week based upon a ransomware attach-were insiders involved? How did the perpetrators get access? Is there coverage?
- As Cyber risks evolve, the need to purchase cyber coverage increases, and if the coverage previously has been purchased, careful underwriting is critical upon each annual renewal.

"Cyber" or "Privacy" Liability Policies:

May Cover:

- *First party costs*
  - Forensic Examination/PCI/ PFI Audits
  - Privacy Notification Costs
    - Privacy counsel
    - Mailing
    - Notification
  - Credit Monitoring/ Call Center Services
  - Public Relations
  - Extortion/Ransomware
- *Third Party Costs*
  - Claims by Private Litigants
    - Consumers
    - Other businesses
  - Claims by State Attorneys General
  - Claims by FTC
  - Regulatory Fines & Penalties
  - PCI Fines & Penalties

May Not Cover:

- Loss of Business
- Damage to Reputation

Note: There is a variation of products in the marketplace. Each policy is subject to its own terms, conditions, limitations, and exclusions.

Considerations for Purchasing Cyber Coverage

- Identification of your risk of exposure
- Involve stakeholders in the purchase renewal process: privacy and other in-house counsel, CIO, CTO—and even the C. CEO?
- Policies are complex with multiple definitions—carefully review to confirm that definitions match business risks.
- ISO exclusions, case law limitations, and evolving risk and associated expenses mean companies need to think about buying specialty coverage.

Cyber Coverage Litigation

- There have been very few cases addressing coverage under "standalone" cyber insurance policies.
- Possible reasons for the lack of cyber coverage litigation:
  - Some companies remain resistant to purchasing standalone coverage
  - Cyber insurance industry is still relatively new, with a lack of uniformity of policy language
  - Apparent (though not quantified) lack of widespread denials of coverage
- As more companies purchase cyber coverage, the amount of cyber coverage litigation will undoubtedly increase.

Are you insured for GDPR and CCPA risks?

- Policy purchase process may need to change
- Large financial exposure for GDPR "fines or penalties"
- Large financial exposure for failure to store or manage data in a GDPR-compliant way
- Insurance policy limits adequate for U.S.-based cyber exposure may not be adequate for GDPR
- "GDPR" language in policy does not guarantee compliance
- Check vendor policies as well

GDPR and CCPA insurance protection

- Companies cannot presume that their current cyber policy will protect against unique exposures arising out of CCPA.
- Many cyber policies cover regulatory exposures, but only with respect to proceedings addressing failures to protect private information.
- Regulators may pursue companies under the Act for broader noncompliant data collection and use practices.

GDPR and CCPA insurance protection

- Third-party claims create the same issue: not all policies cover claims or lawsuits against your company by individuals claiming noncompliance with broader data restrictions imposed by GDPR and the CCPA, particularly when noncompliance does not result in a data breach.

GDPR and CCPA insurance protection

- Some insurers have added "GDPR" language or endorsements to their policies that did not in all instances provide actual GDPR-related protection: endorsements purporting to address the both statutory schemes may not provide as much protection as anticipated.
- As companies are purchasing/renewing cyber policies in advance of CCPA becoming effective, they should carefully scrutinize policy language to ensure that the correct language is included to fortify insurance protection against unknown future financial exposures.