CHAMBERS

Global Practice Guides

Insurance

USA – Trends and Developments

Contributed by

Reed Smith LLP

2018

CHAMBERS® AND PARTNERS

USA

Contributed by Reed Smith LLP

The 'Trends & Developments' sections give an overview of current trends and developments in local legal markets. Leading lawyers analyse particular trends or provide a broader discussion of key developments in the jurisdiction.

Contributed by Reed Smith LLP ***Authors:*** David M. Halbreich, Peter Hardy, Courtney Horrigan, J.Andrew Moss

Trends and Developments

Contributed by Reed Smith LLP

Reed Smith LLP's Insurance Recovery Group, comprised of more than 80 lawyers based in Chicago, Houston, London, Los Angeles, New York, Paris, Philadelphia, Pittsburgh, San Francisco and Washington, DC, is dedicated to representing policyholders - and only policyholders - as an advocate in disputes with insurance carriers and as a counsellor in the purchase of insurance products.

Reed Smith's extensive experience includes virtually every type of property and liability policy ever sold, addressing coverage issues that include commercial crime, kidnap and ransom and fidelity bonds, commercial disputes and intellectual property and advertising injury, commercial general liability, cyberliability, data privacy and security, directors' and officers' liability, employee benefit plan and fiduciary liability, employment practices liability, and many others.

From initial claim review to negotiation, from mediation to all-out, high-stakes litigation or arbitration, our goal in each matter is to achieve the right result and maximum recovery for our clients, with the minimum of expense. From asbestos bodily injury claims, to complex business interruption claims, to false claims act litigation, to copyright, to claims arising out of the fallout of the financial crisis - we have tried them all. We are adept at managing the most complex of facts and boiling them down to their essence. We tell a story the jury can understand. The results speak for themselves. And we do this within negotiated budgets and often pursuant to alternative fee arrangements. We also proactively negotiate policy language and coverage terms to help our policyholder clients avoid costly and lengthy coverage disputes.

The authors recognise the invaluable assistance of Jordan J La Raia, a senior associate member of Reed Smith's Insurance Recovery Group based in its Houston, Texas, office. Jordan focuses her practice on the representation of insurance policyholders in disputes involving directors' and officers' liability, professional liability, cyberliability and commercial general liability.

Authors

David M. Halbreich is a partner and is Global Practice Group Leader of the Insurance Recovery Group. He is experienced in the practice of insurance coverage for: securities fraud claims, fiduciary liability claims, subprime mortgage claims, asbestos and other toxic tort-related claims, environmental/hazardous waste claims, product liability claims, first-party property claims, professional malpractice claims, and construction defect claims. David is a member of the State Bar of California, a member of the American Bar Association, Litigation Section, a member of the committee on Insurance Coverage, and a former co-chair of a Sub-Committee on Alternative Dispute Resolution. He is also a former member of the Committee on Administration of Justice.

Peter Hardy 's experience covers a diverse range of insurance policy types and reflects his particular experience in global, and multi-jurisdictional coverage issues arising in the Financial Services sector in general and disputes under Bankers Bond/ Financial Institutions Combined Liability and Crime policies in particular. Peter has a broad experience of international insurance, reinsurance and Bermuda form arbitrations in London. Peter has acted extensively for financial institutions in respect of losses involving fraud and dishonesty and claims under Bankers Bond, Combined liability insurances, D&O and E&O programmes, in particular where claims arise following regulatory intervention. Peter's claims experience on behalf of banks and financial services companies includes loss and liabilities arising under US securities litigation, mortgage fraud, the operation of offshore-based Ponzi Schemes, computer fraud, bullion theft, payments made under forged instruments, the loss of property held as security, and employee fraud. He is a member of BILA (British Insurance Law Association). Peter has contributed to publications relating to insurance law.

Courtney Horrigan is a partner and deputy head of the Global Insurance Recovery Group. Her areas of practice are insurance coverage for D&O, professional liability, employment practices liability, cyberliability, fidelity and surety bond, fiduciary liability, first person property, general liability, asbestos liabilities, product liability, representations and warranties insurance. Courtney is a member of the Claims and Litigation Management Alliance, and has contributed to insurance law-related publications.

USA TRENDS AND DEVELOPMENTS

Contributed by Reed Smith LLP ***Authors:*** David M. Halbreich, Peter Hardy, Courtney Horrigan, J.Andrew Moss

J. Andrew Moss is a partner in the Insurance Recovery Group. His areas of expertise are insurance coverage for directors' and officers' liability (D&O), professional and errors and omissions liability (E&O), data and network security and privacy liability (cyberliability), fiduciary liability (FLI), employment practices liability (EPL), fidelity bond and commercial crime insurance, and commercial general liability (CGL). Andrew has contributed to publications on the subject of insurance law.

Cybertechnology risks continue to surge into every industry, leaving no sector untouched, whether it be drones and autonomous cars or simply how businesses maintain and share information. As technologies continue to evolve and people continue to find new ways of using (or misusing) them, insurers are developing new, targeted cyberliability policies and insuring agreements to address specific risks, while excluding or narrowing coverage in traditional policies to confine cyberliability risks under specific coverage or for specific industries.

Although policyholders may reasonably assume that a cyber-related liability should be covered by a comprehensive, standalone cyberliability insurance policy, recent claims experience and litigation reveal that the actual risks are less easily defined, that no two breaches are the same and that gaps in coverage may remain. Whether a particular policy will cover a specific cyber-related loss may depend on the terms of the policy and how it interacts with other insurance. Companies should take a holistic approach to risk management. The nature of today's cybertechnology risks means that one insurance policy should not be viewed in isolation and that effective risk management goes beyond the placement of coverage and management of claims. Companies should proactively identify risks and review all policies together to determine where potential gaps in coverage exist (and how to fill them) and determine the company's obligations in the event of a loss or claim. Key personnel and first responders should be educated in the workings of the company's insurance programme and how coverage is triggered in the event of a suspected loss or incident. When developing a holistic risk management strategy, below are just a few of the trends developing in the cyberliability arena that companies should consider.

Beware of "Small Dollar" Cyber Events

Ransomware and cyber extortion are growth areas in cyberliability and cybercrime. Ransomware demands, which may be covered by cyberliability insurance, are often below the retention in a typical cyberliability policy. But ransomware typically enters a company's network in the same manner as other cyber incidents, such as through a phishing e-mail or a sophisticated network intrusion. What if other evidence of an intrusion is later discovered? Cyberliability policies typically have complex notice requirements specifying that incidents be reported during the policy period when the incident was "first discovered" or when it "first occurs." If a later incident occurs – in particular, if it occurs after a policy is renewed – the insurer may assert a late-notice defence if the ransomware event was known but unreported in an earlier policy period. In addition, cyberliability policies often cover the costs of forensic investigations and other professionals, which the company may wish to retain in response to a ransomware attack.

Cyberliability Risks May Include the Physical

Many industries and emerging technologies straddle the physical and non-physical worlds. For instance, a security breach at an autonomous vehicle (AV) or energy delivery network may cause bodily harm and property damage. The breakdown between physical and non-physical risks calls for close attention to the manner in which the company's different insurance policies interact with each other in the event of harm spanning the tangible and non-tangible worlds. Insurers have recently introduced specific policies and endorsements intended to bridge this gap, but the coverage is new and should be reviewed carefully in conjunction with existing insurance.

Attention to Vendor Chain Risks, Indemnification and Contractual Risk Transfer

Many companies use third-party vendors to host and process their data, but does the company's cyberliability coverage respond to a breach occurring at the vendor and involving the company's data? Many current cyberliability forms extend coverage to computer systems operated and information hosted "on the insured's behalf" or "for the insured's benefit," but may require that a written contract exists between the policyholder and the vendor. Insureds should review any (or consider including) contractual defence and indemnity obligations in their agreements with vendors and require vendors to procure their own cyberliability coverage, with specificity regarding the scope of coverage.

Interconnectivity May Equate to Shared Interruption Risks

With the increasing interconnectedness of systems across the world, an attack on one system may be an attack on yours. One recent example is the October 2016 outages in the USA and Europe caused by a distributed denial of service (DDoS) attack on Dyn, which acted as a switchboard for internet traffic. Although not specifically targeted at the theft of data, the Dyn DDoS attack resulted in significant business interruption losses to major online companies, including Twitter, PayPal and Spotify. Including network business interruption

Contributed by Reed Smith LLP ***Authors:*** David M. Halbreich, Peter Hardy, Courtney Horrigan, J.Andrew Moss

(NBI) coverage as a part of a comprehensive cyberliability may be essential if a company's operations are at risk.

Mind the Phishing Gap

Cyberliability policies typically do not cover the direct loss of money or property, even if caused by what most people consider to be cyber events, such as phishing scams, which are at a record high. Many companies purchase commercial crime policies or fidelity bonds, which may include coverage for direct losses due to "computer fraud" or "computer crime." Although these policies may sound like they ought to cover these losses, insurers have argued otherwise, and some courts have agreed. For example, the US Court of Appeals for the Fifth Circuit recently held that a company's losses resulting from paying USD7 million in fraudulent invoices, which had been submitted to an Apache employee through a phishing scam, were not covered by its commercial crime insurance because the payment was authorised by an employee and the e-mail containing the invoices was merely incidental (ie, indirect) to the loss. In a similar case now before the US Court of Appeals for the Ninth Circuit, Travelers is contesting whether its commercial crime insurance policy covers a USD700,000 wire transfer to a person posing as one of the company's vendors, after a senior officer responded to a fraudulent e-mail.

Overlapping or Inconsistent Coverage — Check Your Boiler Machinery Policy

Traditional first and third-party policies may include endorsements intended to provide some degree of protection against security and privacy risks, and in many cases one company may have multiple policies containing cyberliability endorsements. These endorsements may not be tailored for a particular company or insurance programme and may contain provisions that are inconsistent or incompatible with the new comprehensive cyberliability policy the company has purchased. For instance, the endorsements may contain restrictive retention or "other insurance" clauses allowing the insurer to refuse payment until other policies are exhausted. They also may require burdensome obligations on the part of the policyholder, such as the submission of sworn proofs of loss for all claims or losses, or allowing the insurer the unfettered right to take sworn testimony of company officers. At the same time, these one-off security and privacy endorsements on traditional liability policies may offer little to no coverage, leaving the policyholder to fight it out with multiple insurance companies and overcomplicating the claims process.

Although comprehensive cyberliability insurance has become widely available and offered by all the major insurers, a company must take critical steps to make sure that the insurance will actually pay when it is needed. Given all the risks discussed here and other potential pitfalls, companies should (i) review and understand proposed and existing policies carefully in advance of claims, and in conjunction with the company's other insurance coverage, to identify and where possible fix gaps in coverage; and (ii) make insurable risk management a stakeholder in the company's breach response plan so that the company's valuable insurance coverage is not "left on the table" in the event of an incident.

Reed Smith
10 South Wacker Drive, 40th Floor
Chicago, Illinois 60606-7507

Tel: +1 312 207 3869
Fax: +1 312 207 6400
Email: amoss@reedsmith.com
Web: www.reedsmith.com