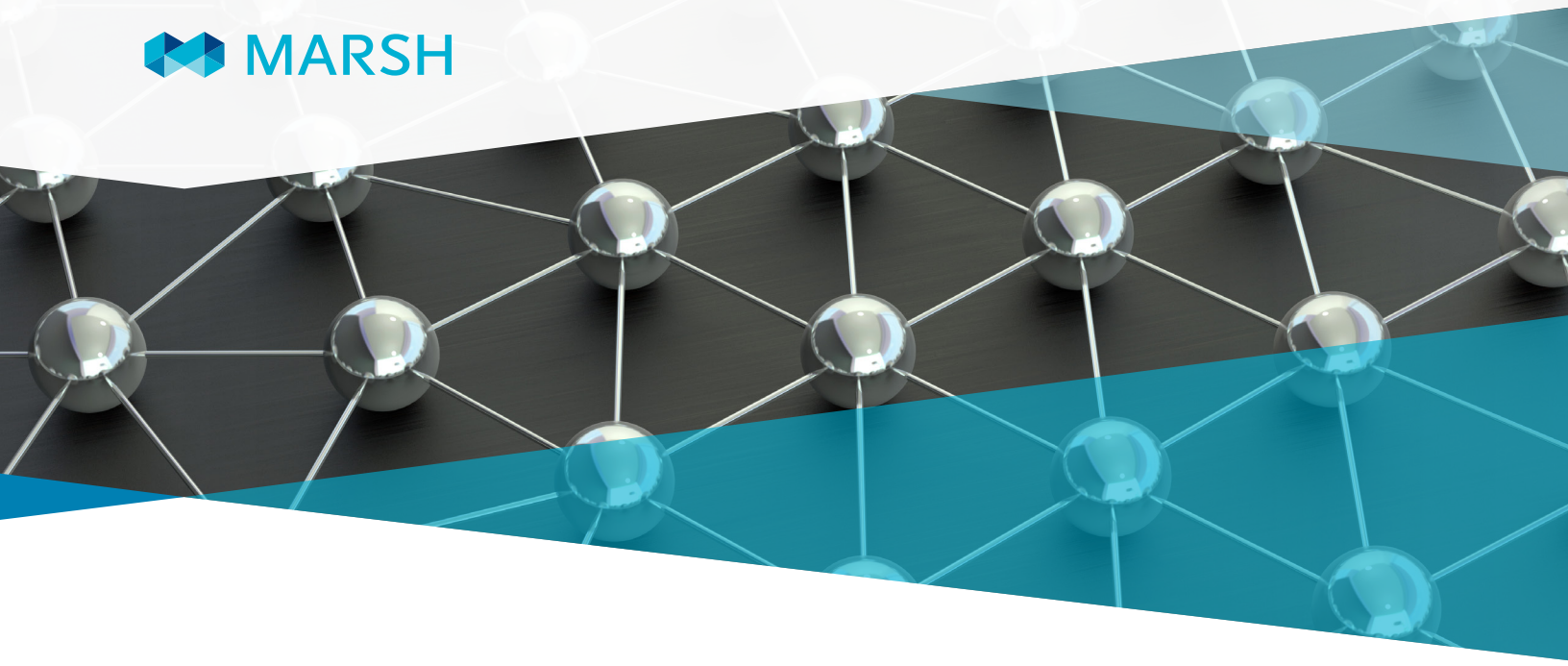
MARSH



The US Financial and Professional Lines Market in 2019: Our Top 10 List

New privacy regulations. An upsurge in workplace sexual harassment claims. Increased securities litigation activity. These are just a few of the risks that rocked 2018. And these exposures are expected to persist, and some will even intensify, in the coming year. As 2018 inches to a close and we ring in 2019, businesses must keep their eyes on the road ahead and the top 10 risk exposures they are likely to face in the coming year.

The Top 10 List:

1. Heightened Securities Class Action Filings
2. The Evolving D&O Market
3. Cyber and Business Interruption
4. Blockchain and Digital Asset Exposures
5. Workplace Worries — The #MeToo Movement and Wage and Hour Woes
6. The Financial Impact of Privacy Regulations
7. Cyber and its Connectivity to Other Policies
8. IoT Devices Increase Security Incident Risks
9. Growing Fintech Industry Faces Increased Regulation
10. Expanded Complexity on a Global Scale

1 Heightened Securities Class Action Filings

The accelerated pace of securities litigation activity — which hit an all-time high in 2017 — continued in 2018. At the end of the third quarter, NERA Economic Consulting projected a total of 416 securities class actions could be filed by the end of 2018, a slight decrease from the 429 filed in 2017. The now-sustained increase in both the number of filings and average and median settlement amounts, continues to cause concern for the defense bar and insurers alike. This trend is expected to persevere in 2019.

Merger objection cases remain a driving force behind the increase in filings. Although the rate of increase in such filings has slowed, the costs associated with defending mergers and acquisitions (M&A) litigation is on the rise.

The event-driven securities class action phenomenon, while only representing a fraction of total filings this year, is one to watch. Event-driven securities class actions occur when an adverse event at a company triggers a securities claim. In many of these cases, the underlying litigation is brought by injured consumers, employees, or others, generally based on some type of alleged tort. In these cases, a D&O claim usually arises after a stock drop takes place and allegations typically involve some type of failure to disclose or misrepresentation at the corporate level or because of an alleged breach of a fiduciary duty, both surrounding the allegations in the underlying litigation. Common examples of event-driven D&O claims involve those arising out of the #MeToo movement and cyber/privacy breaches.

The US Supreme Court's 2018 decision in *Cyan Inc., et al v. Beaver County Employees Retirement Fund, et al* will undoubtedly lead to a shift in filings in years to come. Under *Cyan*, Securities Act of 1933 claims can be filed in either federal or state court. The implications of *Cyan* extend beyond companies going public in an initial public offering, as any public company issuing stock — or using stock as a currency in a merger or acquisition situation — can face litigation in both federal and state courts. *Cyan* will undeniably be a catalyst for class action litigation attorneys to search for the most plaintiff-friendly jurisdiction and thus introduce forum-shopping and inconsistent standards across multiple jurisdictions. Defense costs and settlement values are also expected to increase as a result of the decision.

All of these trends, and the overall increase in filings, are being closely watched by the D&O industry. The increase in filings, and subsequent losses, have, in large part, led to the gradual firming of the D&O market, as discussed later in this document.

2 The Evolving D&O Market

In the third quarter of 2018, primary and total program pricing for directors and officers liability insurance increased for the third consecutive quarter. This year was the first time since the first quarter of 2014 that total program public company D&O pricing had seen an increase.

Due to continued deterioration in loss activity, we expect D&O insurers to remain focused on profitability by way of increased rates. Generally speaking, we anticipate continued pressure on primary, excess, and even Side-A premiums. Some insurers have warned that this will not necessarily be a one year "restoration" or "correction" of price increases. We expect to see low excess layers — those within the first $50 million in limits and especially first excess layers — seek more significant rate adjustments. Other excess layers at higher attachment points will also likely continue to put pressure on rates.

Further, we expect D&O insurers to remain willing to walk away from business, or reduce capacity, if they are not getting the pricing they need. Insurers will likely be less inclined to negotiate policy wording requests and enhancements. Overall, capacity remains abundant, but available only at the "right price."

In addition, in a gradually firming D&O market, insurers will likely take more aggressive coverage positions and more strictly enforce certain policy provisions. While insurers have often granted clients somewhat liberal policy interpretations and paid claims in the past, they may take a more conservative view and deny substantially similar claims going forward. Insurers will be more likely to take a harder stance on late notice issues, incurring defense costs without prior consent, and interrelatedness issues, to name a few. We expect to see more claim denials for noncompliance with technical policy provisions and more deductions of defense costs for noncompliance with litigation guidelines. The anticipated shift in insurer claims behavior highlights the importance of understanding the claims reputation of each insurer on your program, each insurer's ability to shape the tenure of coverage discussions in connection with a claim, and the value that long-term insurer partnerships can play.

3 Cyber and Business Interruption

Business interruption has become a preeminent cyber risk, viewed on par with natural disasters. In mid-2017, a large-scale global attack that used a variant of an earlier ransomware known as NotPetya, encrypted files on computers around the world. Recent analysis by Property Claims Services estimates that aggregate

insured losses from NotPetya now amount to $3 billion across multiple lines of coverage, and could climb further. In response, clients are proactively seeking risk transfer for cyber business interruption risk. Business interruption insurance coverage continues to evolve, including expansions for supply chain and receiver interruption and mirroring the traditional property approach to calculating loss.

4 Blockchain and Digital Asset Exposures

Whether by miners, custodians, advisors, incubators, exchanges, or companies going through initial coin offerings or other types of offerings, the use of blockchain technology and/or digital assets is undoubtedly here to stay. With the regulatory environment expected to continue to evolve in 2019, both startups and more established companies will continue to make significant investments in this space.

Insurers have traditionally been reluctant to provide coverage to this newer risk class, due, in part, to sensationalized press reports about blockchain and other digital assets. As Marsh's Digital Asset Risk Transfer (DART) team continues to devote a significant amount of time to educating the insurance market about this industry class, we expect to see an increase in the number of financial and professional lines insurers who are willing to provide broad coverage to our DART clients at a competitive price in 2019. In addition, we expect alternative risk transfer options to play an increasingly significant role in this space.

5 Workplace Worries — The #MeToo Movement and Wage and Hour Woes

The rise of the #MeToo movement has put a spotlight on sexual harassment in the workplace. While these types of claims have been prevalent for years, the new attention has led to an increase in reports. According to the Equal Employment Opportunity Commission (EEOC), sexual harassment charges filed by employees increased 13.6% in fiscal year 2018, which ran from October 2017 through September 2018, when compared to the prior year. Further, the number of sexual harassment lawsuits brought by the EEOC itself also increased by more than 50%.

Employers have experienced an increase in internal complaints, as well as attorney demand letters alleging sexual harassment, and state employment agencies have noted an uptick in charge filings. This suggests that there are a significant number of claims not captured by EEOC data. Further, the management and settlement of claims has become more expensive and complicated, in part due to new laws designed to discourage or prevent nondisclosure provisions in settlement agreements and mandatory arbitration of harassment claims. These difficult claims have already had a significant impact on the employment practices liability (EPL) market, and are beginning to affect the D&O market as well. With no sign of abating in the near term, sexual harassment will likely be an issue that employers will need to wrestle with for years to come. In the era of #MeToo, businesses should be prepared to address employment-related policies during their next D&O underwriting meetings.

Additionally, there is no decline in litigation regarding wage and hour issues, such as failure to pay overtime, failure to provide meal/rest breaks, and misclassification of employees. In light of dynamic standards at both the state and federal level, joint employment relationships affecting both EPL and wage and hour, are an exposure threat most companies face today. The federal standard governing joint employment has remained in flux for a number of years, and many states utilize their own "test" to determine if a company is functionally a joint employer. Recently, certain states have also taken their own initiatives to hold "upstream" employers liable for the employment violations of "downstream" companies those employers contract with. Coverage can be designed to address this developing risk, with policies that feature bespoke manuscript wordings and endorsements to address the unique risks faced by each individual insured.

6 The Financial Impact of Privacy Regulations

The EU General Data Protection Regulation (GDPR) came into effect in May 2018 with wide-reaching provisions that revolutionized the data protection landscape worldwide, requiring subject companies to review and enhance their privacy and data protection practices, or face significant fines, penalties, and other costs. Although most insurers now offer coverage for fines and penalties related to noncompliance, it is still unclear whether such damages are insurable. EU officials have advised that the first round of fines and other disciplinary actions are expected soon, meaning that 2019 will likely see more activity on this front, which will in turn provide more clarity on how carriers treat related claims.

Many US companies will also need to comply with a new privacy law enacted in California in June 2018. When it takes effect in January 2020, the California Consumer Privacy Act (CCPA) will be the most stringent and comprehensive piece of data protection legislation in the US. Like the GDPR, companies that are noncompliant with the CCPA may be investigated and face significant fines. Most markets have not yet committed to covering CCPA penalties, although we expect insurers to adopt a similar position as they have with the GDPR, so long as sufficient underwriting information is provided.

Privacy regulation exposures are not just limited to cyber insurance related losses. In fact, we have already seen D&O-related activity arise out of privacy regulation violations. Accordingly, it is imperative that you work with your insurance advisor to ensure you have the appropriate coverages in place to best protect your company and its directors and officers.

7 Cyber and its Connectivity to Other Policies

Privacy is a top board concern for most companies, but cyber coverage is not the only policy that can be triggered during a privacy or cyber event. If an employee's privacy rights are violated by an employer — for instance, through alleged inappropriate biometric screening — coverage may be triggered under an EPL policy. If a hacker intercepts emails and convinces an employee to wire money for an acquisition that is not in fact occurring, it could be considered a crime loss. If a hacker steals data and demands a ransom in order to return it safely, kidnap and ransom coverage could apply. A cyber incident could lead to allegations of corporate or C-suite level misconduct and therefore could trigger coverage under a D&O policy.

The crossover between these types of claims requires a total program review of all of your company's insurance policies, and how they interplay, in order to understand the true scope of coverage.

8 IoT Devices Increase Security Incident Risks

Industrial control systems, smart buildings and homes, pacemakers, cameras, and even fish tanks — all of these Internet of Things (IoT) products have been hacked by cyber-attackers looking to disrupt networks and extort money from users. As cyber criminals increasingly use IoT devices as a gateway to larger computer networks, the companies that manufacture these connected products face significant risks. The myriad of connection points and collection of confidential data creates increased severity potential for security incidents, privacy events, product risk, intellectual property risk, and cyber extortion. As a result, manufacturers that historically may not have had such direct technology risk, need to rethink how they structure network security solutions, including an investment in risk transfer.

9 Growing Fintech Industry Faces Increased Regulation

Fintech companies continue to disrupt the financial services industry, changing how individuals invest, borrow, and save; how banks control risk; and how hedge funds analyze data and select their investments. Worldwide, investments in Fintech startups increased steadily between 2014 and 2017, from $19.9 billion to $39.4 billion, and accelerated in the first half of 2018 when $41.7 billion was invested across 789 deals, according to Fintech Global.

Fintech companies face complex and varied risks stemming from their increased use of technology and data in the delivery of products and services previously provided by traditional financial institutions. As the Fintech industry continues to grow, the regulatory spotlight on the sector is expected to intensify. Fintech companies, currently subject to some of the same consumer and investor protection regulations as traditional financial institutions, must balance compliance requirements with the need to innovate, grow, and develop new products. Cyber and privacy risks can also contribute to significant economic loss and reputational damage.

The risk profiles of Fintech companies don't fit into the traditional categories insurers underwrite, which means it's often difficult for these companies to find adequate and cost-effective insurance

solutions. To address this challenge, Marsh — together with Validus Specialty — developed FINTECH Protect, an insurance solution that provides comprehensive financial protection against management, professional, employment, and cyber liability risks, and broad coverage for direct losses associated with theft, computer crime, extortion, data breach, and technology failure. Its broad, proprietary policy wording is designed to address the varied and dynamic risks of privately held fintech companies, including those backed by venture capital and private equity funds, and is one way in which to transfer risk associated with the increased regulation.

10 Expanded Complexity on a Global Scale

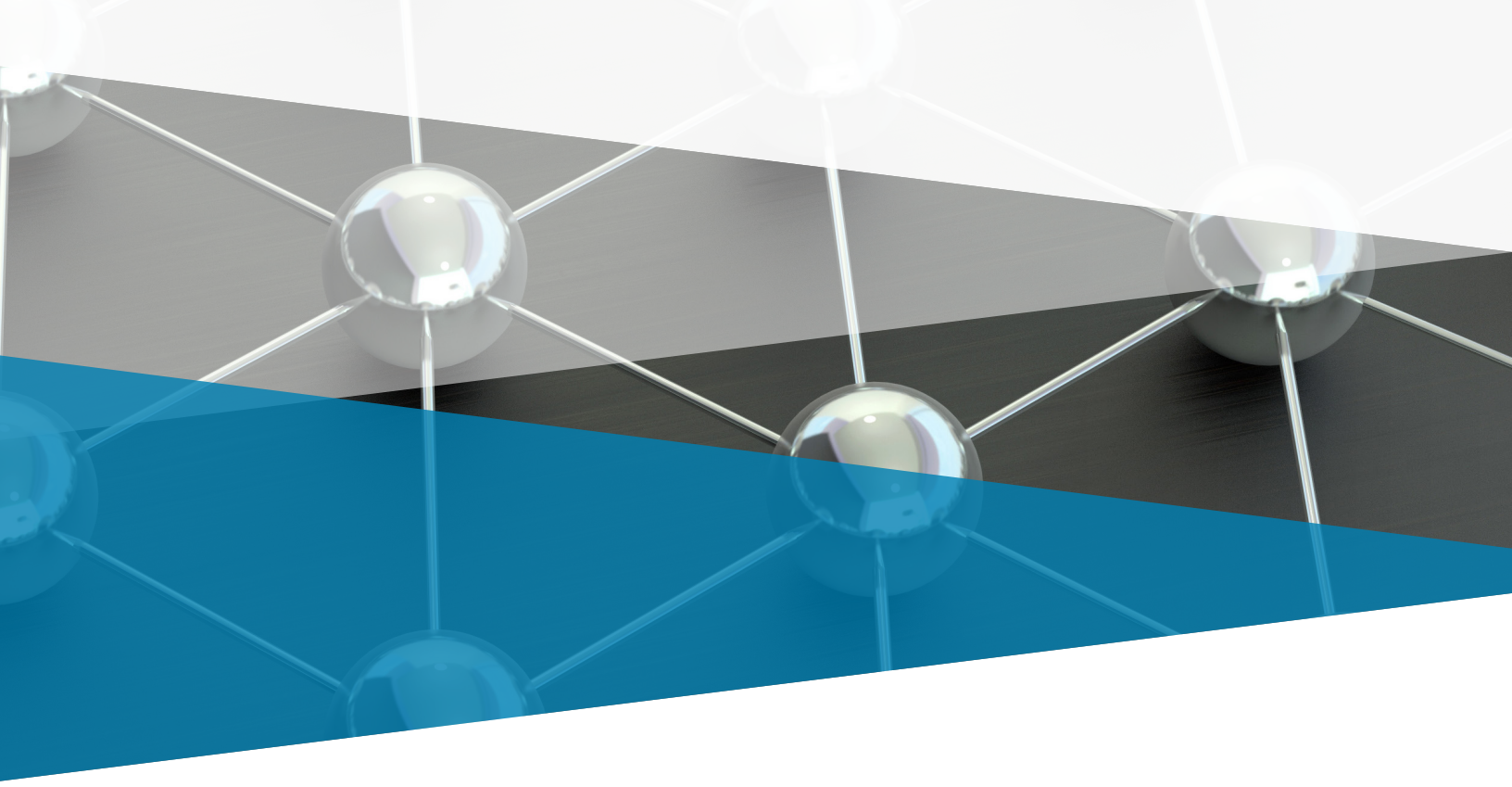
As companies continue to expand their operations to reach diverse customers outside the US, whether physically or via the internet, they face an increasingly challenging legal and compliance landscape. Over the past several years there has been a steady resurgence and escalated enforcement of anti-corruption laws around the world. From Brazil to France, anti-corruption scandals have resulted in several million dollars in fines, often because of multi-jurisdiction cooperation. Most notable were Telia's $965 million settlement, shared by US, Swedish, and Dutch regulators, and Société Générale's $585 million settlement, split between the US and France.

In addition to hefty fines, companies could also face shareholder actions. For example, Wal-Mart recently announced a $160 million settlement relating to a 2011 Foreign Corrupt Practices Act investigation that cost the company well over $800 million in internal investigations and compliance improvements. Class action litigation, meanwhile, has become a real threat outside the US. Higher demands for transparency and increased scrutiny over employment practices, consumer protections, and privacy rights have prompted regulatory action in several countries.

Following a security hack, cryptocurrency exchange Coincheck was sued by consumers under Japan's new class action system, while also prompting regulatory action from Japan's Financial Services Agency. Similarly, regulators in Australia have initiated an inquiry into misconduct in the country's banking and finance industries. And the extraterritorial reach of the recently enacted GDPR has expanded data security and compliance responsibilities for companies and their directors and officers, who can be held personally liable.

Finally, the rise in popularity of protectionist trade policies and sanctions — such as the re-imposed sanctions against Iran, and the United Kingdom's March 2019 withdrawal from the European Union — have made operating outside the US more complex. Organizations and their directors and officers must tread carefully even when navigating jurisdictions in which they are familiar.

The coming year is sure to bring some surprises. But we don't need a crystal ball to tell us that some of these trends will continue and may even worsen. As 2018 winds down and we enter the new year, it is imperative to keep in mind that many of the unfavorable developments in the financial and professional lines market have not existed in more than a decade. These changes are a result of the perfect storm effect of some of the trends discussed above and make it more important than ever to begin insurance coverage strategy discussions well in advance of your renewal.



For more information, visit marsh.com, contact your Marsh representative, or contact:

DEVIN BERESHEIM
Practice Leader
Marsh FINPRO
+1 212 345 5062
devin.beresheim@marsh.com

CAROLE LYNN PROFERES
Product and Industry Leader
Marsh FINPRO
+1 215 246 1105
carolelynn.l.proferes@marsh.com

SARAH D. DOWNEY
Directors and Officers Liability
Product Leader
Marsh FINPRO
+1 212 345 3122
sarah.d.downey@marsh.com