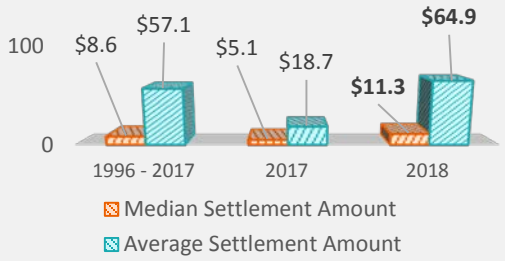
2019

EXECUTIVE LIABILITY
Market Update

"Am considering taking Tesla private at $420. Funding secured." – @elonmusk. August 7, 2018. Twitter

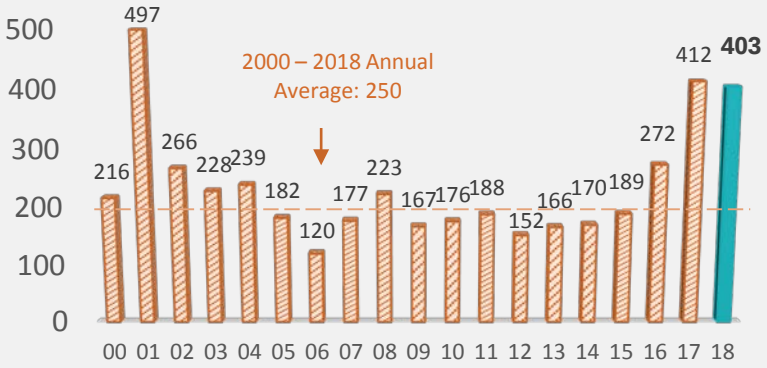
DIRECTORS & OFFICERS LIABILITY

AVERAGE AND MEDIAN SECURITIES CLASS ACTION **SETTLEMENT AMOUNTS**



- Total settlement amount increased to over $5 billion in 2018, up from $1.5 billion in 2017.
- 5 securities class actions settled for more than $100 million.

SECURITIES CLASS ACTION **ANNUAL NUMBER OF FILINGS** 2000 -2018



- **HERE A SUIT, THERE A SUIT, EVERYWHERE A LAWSUIT.** SUPREME COURT ALLOWS FOR CONCURRENT JURISDICTION IN § 11 FILINGS. On March 20, 2018, the Supreme Court ruled unanimously in *Cyan, Inc. v. Beaver County Employees Retirement Fund* that class actions under the Securities Act of 1933 may be brought in state courts, thus making securities class actions, including IPO-related actions, more difficult (and more costly) to defend. Claims under § 11 of the 1933 Act, which generally assert false or misleading statements in initial public offerings, are often brought in conjunction with related claims under § 10(b) of the 1934 Act. While the § 11 claim may be brought in either federal or state court, the § 10(b) claim has exclusive federal court jurisdiction. Thus, cases in federal court and potentially multiple state courts may not be consolidated, and defendants' historical strategy of filing a motion to dismiss, and settling if the motion is not successful, is no longer possible. Rather, securities class actions will require actual litigation. With fears of increased costs associated with the defense, *Cyan* firmed the D&O market for IPO-related risks virtually overnight. **BUYER BEWARE!** If the plaintiffs' bar can trace share issuance to a registration statement associated with an announcement of a planned purchase of another company, this concurrent jurisdiction problem may also arise in M&A litigation.
- **FIRST COMES A TWEET, THEN IT GOES VIRAL, THEN COMES A LAWSUIT ALLEGING MISMANAGEMENT.** EVENT SPECIFIC LITIGATION SKYROCKETS. Events unrelated to the financial condition of a company have resulted in filings in 2018. Known as Event Specific Litigation, these lawsuits are hard to predict as they tend to be operational or reputational in nature, such as suits arising out of social media posts by outspoken CEO's, the #metoo movement or California wildfires. As we have seen with Marriott and Facebook, other examples include D&O and data recovery lawsuits arising out of cyber-related events.
- **THE NEW NORMAL.** MERGER OBJECTION SUITS IN FEDERAL COURT. Merger objection suits, or M&A filings, account for 185 of the 403 (46%) federal securities class action filings in 2018. This uptick continues the trend that began in 2016 following the Delaware Court of Chancery's decision in *Trulia,* in which the court acknowledged merger objection claims bring little value to shareholders, thus leading plaintiffs' attorneys to seek more favorable venues – often federal courts. Despite the filing uptick, the percentage of M&A filings against transactions valued over $100 million are beginning to fall. And although still significantly higher than average, suits against the consumer non-cyclical industry decreased in 2018 with 31% of all core filings made against Biotechnology, Pharmaceuticals and Healthcare, as compared to 40% in 2017.

FUN FACTS. SO YOU'RE SAYING THERE'S (EVEN MORE OF) A CHANCE….

Likelihood a public company is subject to a core filing (non-M&A):

4.5%

With the number of publicly traded companies decreasing and overall filings increasing, 2018 marks the 6th year in a row of a percentage increase (up from 2.6% in 2012).

# of core filings (non-M&A) by industry (2017 figure in parenthesis):

Energy: 7 (9)
Financial: 19 (20)
Consumer Non-Cyclical: 68 (85)
Industrial: 20 (26)
Technology: 22 (14)
Utilities: 3 (2)

Core filings (non-M&A) dismissal rate:

58%

The highest dismissal rate on record.

 # State Court 1933 Act Filings:

30

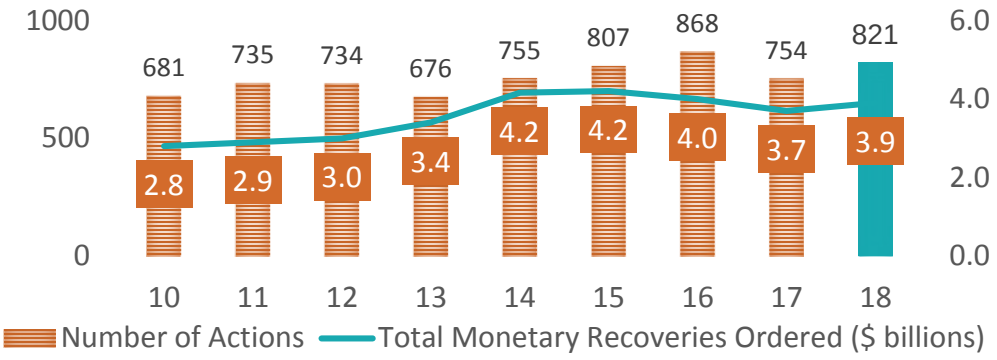
An 88% increase from 16 in 2017 and 200% increase from the 2010 – 2017 average of 10. Most of the suits were filed in California (16) and New York (13).

Likelihood of litigation against recent IPOs (2009 – 2017) within four years of the IPO:

19.5%

DIRECTORS & OFFICERS LIABILITY

SEC ACTIONS AND MONETARY RECOVERIES



- 490 of the 821 actions were stand alone actions brought in federal court or as administrative proceedings. Roughly 25% of the stand alone actions concerned securities offerings.
- $1.43 billion in recoveries represent penalties whereas $2.5 billion represent disgorgements.
- Of the $3.9 billion recovered, $1.78 billion came out of the Petrobras bribery action.

- **LACK OF CTRL. SEC'S FOCUS ON CYBER.** On October 17, 2018, the SEC issued a statement reminding public companies of the importance of internal controls in the prevention of cyber fraud. Although the SEC's Enforcement Division has investigated several public companies, it has not brought an enforcement action against a company for lack of internal controls. It did, however, bring its first enforcement action relating to failure to disclose a cyber breach. In this action, Yahoo! paid a $35 million penalty after the SEC found the company failed to properly assess the scope and impact of the breach and failed to properly inform investors about the breach – one of the largest in history.

  With 125 active cyber-related investigations, the SEC's focus is clearly on cyber disclosures, and although the SEC has issued a warning to public companies, do not expect it to penalize every company falling victim to a cyber breach. The agency did, after all, experience a highly-publicized breach of its own.

- **SLOW START, FAST FINISH. SEC ENFORCEMENT ACTIONS AGAINST PUBLIC COMPANIES INCREASE IN THE SECOND HALF OF THE YEAR.** After recording the fewest enforcement actions against public companies and their subsidiaries in the first half of 2018 (15), the SEC filed a record-breaking 55 actions in the second half, bringing total filings to 71 – a 9% increase over 2017 (65). Individuals of public company defendants were named in 23% of all the actions, with CEO's and CFO's being the most commonly named. Speaking of individual accountability….
- **"INVOLVED" EVOLVES TO "SUBSTANTIALLY INVOLVED". NEW YATES MEMO STANDARD.** In a November 29, 2018 speech, U.S. Deputy Attorney General Rod Rosenstein shed light on the Trump administration's stance on the Yates Memo. Though the Memo originally encouraged companies to identify any and all persons who may have been involved in potential wrongdoing, the DOJ is now taking a softer tone. In an attempt to curb concerns about wasted resources, Mr. Rosenstein announced that going forward, companies must identify only individuals who were substantially involved in potential wrongdoing in order to receive a cooperation credit .
- **EXECTIVE COMPENSATION UPDATE.** In its In re Investors Bancorp, Inc. Stockholder Litigation decision, the Delaware Supreme Court held that, except under limited circumstances, it will not apply the business judgment rule (and assume good faith) in reviewing challenges to director compensation awards granted pursuant to stockholder-approved equity plans. Instead, such awards will be subject to an entire fairness standard of review. This decision is significant because plaintiffs are more likely to defeat a motion to dismiss, potentially costing the company substantial sums in litigation and discovery.

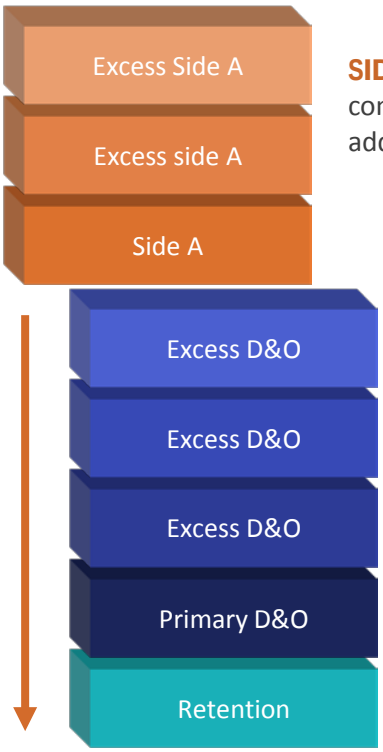
DIRECTORS & OFFICERS LIABILITY

The Monty Python Black Knight reference seems appropriate when painting the picture of the current state of the D&O market – years of low premiums have cut off one arm while an increase in claims has severed the other. In order to stop the bleeding, carriers have begun taking a tougher stance on recent renewals especially on a program's lower layers. In a report released by Trans Re in October 2018, overall pricing in the D&O market has decreased 15% from 2013, with the greatest premium erosion occurring in the higher excess spots. In addition to low premiums, there has been an increase in claims as both securities class action filings and derivative actions have seen an uptick. The result of this perfect storm has led underwriters to take corrective actions in order to survive.

The most significant announcement about profitability came from AIG on Thursday, February 14, 2019. During its 4th quarter earnings call, AIG announced a substantial increase in loss reserves. Of the reserve adjustment, $362 million is attributed to unfavorable primary and excess D&O and employment practices liability results, particularly in 2016 and 2017.

AIG is not alone as several other D&O insurers have experienced adverse loss development, although the magnitude of such negative development for these insurers remains to be seen. We expect the market to experience consistent upward D&O premium pressure and greater underwriting scrutiny. Unlike past years, underwriters are seeking rate increases on many stable, profitable, claim-free accounts. Those of us who have experienced "hard market" conditions know this: with very few exceptions, the increased rates and greater scrutiny are due not to hard market conditions but to a very intentional push to achieve greater underwriting discipline and rate adequacy. Accounts that have seen year-over-year rate compression will likely see underwriters seeking to recoup rate. Most insurers, so far, have been willing to differentiate rate increases for accounts that have maintained year-to-year premium stability.

NOT ALL LAYERS ARE CREATED EQUAL



SIDE A. The market for Side A only layers continues to remain soft to stable. If comfortable with the risk, some carries participating lower on a program may request additional Side A only capacity as a way to balance their overall portfolio.

EXCESS D&O. Historically viewed as the most profitable layer on a D&O program, the premium on the first excess layers have taken a nose dive over the past several years. With an increase in number of claims and settlement amounts, the first excess D&O layer is now considered one of the least profitable layers. In addition to premium, carriers are now concerned about the amount of limit exposed on any one risk with some carriers only willing to write layers of $10 million. Many recent renewals have seen the first excess receive a greater increase from a percentage standpoint than the primary.

PRIMARY D&O. Over the past several years, newer entrants into the D&O market grew their book by writing primary layers despite not having a book to absorb losses. There is now less competition on the primary layers causing an increase in rates.

RETENTION. Expect pressure from primary carriers to increase retentions especially for certain industries (e.g., Life Science) and IPO placements.

"Cars with flames painted on the hood might get more speeding tickets. Are the flames making the car go fast? No. Certain things just go together. And when they do, they are correlated. "— Barbara Kingsolver

DIRECTORS & OFFICERS LIABILITY

In October 2018, the EY Center for Board Matters released a report that analyzed public filings of Fortune1000 companies for cybersecurity-related disclosure practices. Below are the highlights from the report

CYBERSECURITY DISCLOSURE BENCHMARKING

BOARD OVERSIGHT

- 84% disclosed that at least one committee was charged with cybersecurity oversight.
- 70% stated that the audit committee oversees cybersecurity matters.
- 41% identified cybersecurity experience as among key director qualifications considered by the board.
- 41 described how management reports to the board about cybersecurity.
- 34% disclosed the frequency of management reporting to the board.

CYBERSECURITY RISK MANAGEMENT

- 71% of companies described efforts to mitigate cybersecurity risk such as investing in personnel, training and monitoring.
- 30% referenced response planning, disaster recovery or business continuity considerations.
- 3% identified preparedness including simulations or tabletop exercise.
- 15% disclosed the use of education and training.
- 5% disclosed collaborating with peers, industry groups or policymakers.
- 14% reported the use of an external independent auditor.

Is there a correlation between cyber events and D&O claims?

CYBER CORRELATION

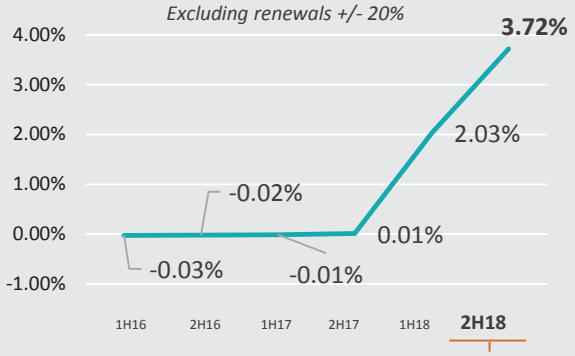
- In a Georgetown University study of Market Implications of Data Breaches, researchers concluded that the announcement of data breaches does not have a meaningful impact on the volatility of equities across industries and does not meaningfully depress stock longer than a week.
- From 2014 to 2016, D&O claims were typically brought as derivative actions and were often unsuccessful due to broad protections of the business judgment rule.
- Post 2016, claims have been brought as securities class actions, and with the exception of Yahoo! ($85 million settlement and $35 million SEC fine), have generally been unsuccessful.
- In the past 12 months, there has been an increase in cyber-related securities class actions. Where we see scienter and long-term depression of stocks, we expect a correlation between the cyber event and the securities class action.
- Although it remains unclear whether cybersecurity disclosures increase the risk of suit, the additional disclosures could provide the plaintiffs' bar with ammunition for scienter claims.

PURCHASING TRENDS

(Based on McGriff FSD public company 2H 2018 renewals)

% CHANGES IN PRIMARY PRICE PER MILLION

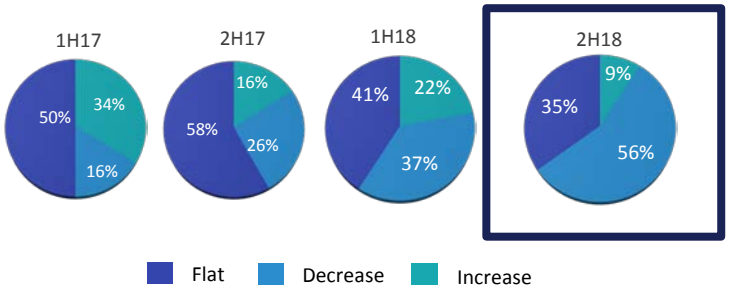
Excluding renewals +/- 20%



19% of all 2H 2018 D&O renewals received increases of greater than 20% (thus not calculated in the above). This is a 12% increase over 1H 2018.

% OF RENEWALS WITH CHANGES IN PRIMARY PRICING

All renewals



CYBER RISK

STATE OF THE MARKET

Predicted to grow from $4.2 billion in 2017 to $22.8 billion in 2024, the global cyber market continues to attract carriers with broad risk appetites and coverage terms. The competitive marketplace has led to innovative coverage solutions specific to an insured's risk profile as well as greater value-add services such as risk quantification models. Market growth comes despite increases in regulatory actions and claims, such as ransomware and security breaches. As capacity expands, the market continues to mature in the following ways:

- **Coverage Breadth.** To differentiate themselves from the competition, some carriers will extend business interruption coverage to incidents at third party technology service providers. Others will extend the contingent suppliers / dependent business interruption coverage to non-technology business service providers. But the broadest coverage extends business interruption coverage not only to any failure of the insured's systems but also to system failures at any technology or non-technology service providers, essentially insuring the insured's total supply chain. This coverage is not available for all industries nor could it be characterized as market standard, although we anticipate more carriers may offer if the price and retention are appropriate. The sustainability of this breadth of coverage is uncertain, especially as underwriters manage their aggregation risk.

- **Program Coordination.** Because multiple lines of coverage may be impacted by a single cyber event, such as a ransomware attack, P&C insurers and their reinsurers have reconsidered their overall exposure and have developed new products aimed at extending coverage to "silent cyber" exposures. Where policies do not have clear cyber exclusions, carriers fear they may be insuring more cyber-related losses than they considered when underwriting traditional P&C exposures. Reinsurers are insisting that primary insurers better evaluate their cyber exposures and clarify which cyber risks are actually covered. We expect this pressure to increase in 2019 and likewise expect non-cyber insurers to begin asking cyber-specific underwriting questions, followed by narrowing exclusions and new cyber sublimits. Alternatively, several P&C carriers have begun offering buy-back features to their General Liability and Property policies, removing cyber-related exclusions in the respective policies.

- **Risk Quantification.** With business interruption losses getting front page attention, companies understand that data breaches are not the only losses to worry about. Risk managers and other insurance buyers are employing data analytics and cyber risk quantification models to comprehensively assess their cyber threat landscape and the impact of threats on their balance sheets. Abundant tools are available to perform this quantification exercise, but buyers should be cautious in relying on them. Many models use past loss statistics to predict the likelihood and severity of cyber attacks on an organization, but this approach does not adequately adjust for new attack methods. None of these models would have predicted WannaCry or NotPetya and most would not have recommended cyber insurance limits in excess of $200 million. We propose a vulnerability-based risk analysis of a company's actual technology footprint. This technique, combined with advanced cost analytics and machine learning, can generate a maximum probable cyber loss range specific to the organization in question.

CYBER RISK

HOT TOPICS

RANSOMWARE ATTACKS OF 2017 SEND SHOCKWAVES THROUGH THE INSURANCE INDUSTRY

WAR & TERRORISM EXCLUSION TRIGGERED?

PROPERTY INSURANCE: BI/EE CYBER TRIGGER

PROPERTY DAMAGE LOSSES, EMERGENCE OF "BRICKING" COVERAGE

Following the impact of the 2017 NotPetya "destructive wiper worm," Mondelez Corporation (Nasdaq: MDLZ) sued its property insurer Zurich American Insurance for $100 million in recovery under its all-risk property insurance policy following Zurich's refusal to provide coverage for physical damage suffered to electronic data, programs and software, including malicious introduction of a machine code or instruction, which rendered over 20,000 laptops and servers "permanently dysfunctional." According to the complaint, the claim was on a seemingly predictable course, with Zurich evaluating Mondelez's proof of loss substantiating its financial damages, when Zurich abruptly changed its posture from coverage negotiation to full denial based on the policy's war exclusion– "hostile or warlike action in time of peace or war…by any government or sovereign power." It is believed that Russian military hackers are behind NotPetya, which took advantage of a known vulnerability in the tax/accounting software used by the Ukrainian government and local businesses, thus allowing the hackers to hijack servers at a Ukrainian accounting firm and gain backdoor access to PCs around the country. Even if Zurich proves that NotPetya falls within the war exclusion, can we rely on government finger pointing? According to cybersecurity experts, it is very hard if not impossible to verify where attacks originate.

REGULATORY OVERSIGHT INCREASES

Since implementation of the General Data Protection Regulation (GDPR) on May 25, 2018, European regulators have reported over 59,000 data breach notifications by public and private organizations. The much anticipated regulation was created to protect individuals within the European Union (EU) by confirming individual consent to collection and storage of personal data and requiring companies to store the data with anonymization using high privacy settings. GDPR applies to any business who processes personal data in an EU establishment or offers goods and services to EU individuals, and failure to comply with the regulation may result in a penalty of up to 4% of global revenue. According to a survey by DLA Piper, the Netherlands leads the way in breach notifications with approximately 15,400, followed by Germany and the United Kingdom with 12,600 and 10,600 notifications, respectively. Ireland comes in a distant fourth with 3,800 disclosures, according to the survey. And the award for largest penalty imposed by regulators so far goes to…..Google at $57 million. The insurability of GDPR fines and penalties has been an area of considerable discussion in the insurance community as civil fines and penalties are uninsurable in many jurisdictions. Policyholders should review their cyber policies to determine whether coverage extends to civil fines and penalties and to understand which jurisdiction governs policy terms and conditions.

CYBER RISK

THE YEAR OF THE M&A MEGA BREACHES: MARRIOTT / STARWOOD & VERIZON / YAHOO

Marriott / Starwood

In 2016, Marriott acquired Starwood Hotels and Resorts including Starwood's guest reservation system – the largest in the world. Unbeknownst to Marriott, the reservation system was breached in 2014 and remained under an active hacking campaign. The reservation system breach was discovered in 2018 and affected 383 million records (multiple records per guest), including encrypted credit and debit card numbers and both encrypted and unencrypted passport numbers. Marriott does not know whether hackers also stole the decryption keys (i.e., code necessary to decrypt the encrypted data sets). In response to the breach, Marriott set up call centers in 55 countries, established fraud centers to assist customers with fraud claims in 3 countries, and sent email notifications to affected guests. Marriott purchases cyber insurance, and we expect a portion of the program to respond. The oversight of the breach during Marriott's acquisition of Starwood may increase overall awareness of such risks during M&A due diligence.

Yahoo! / Verizon

While in negotiations to sell to Verizon in 2016, Yahoo! announced a massive breach of its user database dating back to 2014. Prior to the announcement, Yahoo! stated in its public filings that it was not aware of any security breaches. However, Yahoo! was aware of the breach, and had been aware since 2014, but it did not understand the extent of the breach until it began an investigation of a separate breach in July 2016. Ultimately, 3 billion users were impacted, and a slew of breaches were discovered in Yahoo! systems. Yahoo!'s failure to discover and report the breaches resulted in much criticism and settlements with users. As a result of the breach, Verizon lowered its purchase price by $350 million. Additionally, Yahoo! settled breach-related derivative securities suits for $29 million and $80 million, respectively, and paid a $35 million SEC penalty.

FEEDING THE BEAST. MORE THAN 50% OF RANSOMWARE DEMANDS ARE MET

WHAT? Ransomware is a malicious software (malware) that locks up a victim's systems and demands a ransom – often in cryptocurrency – in order for the victim to regain access to its systems and data. Unlike other forms of cyber crime, ransomware causes the victim to lose access to its systems, potentially disrupting operations.

HOW? Most ransomware infections come from phishing attacks in which unaware users are enticed to open a file or click on a link containing the ransomware malware. The payment of a ransomware demand does not guarantee the attacker will provide the right encryption key for the victim to be able to access the data.

WHY? Easy, Peasy + Law of Large Numbers = Successful Day at the Office. The relatively low requisite skill set coupled with the ease of sending voluminous phishing emails makes ransomware popular. Large numbers of ransomware demands have inundated law enforcement, forcing them to prioritize demands based on monetary amounts.

HOW MUCH? In 2017, Ransomware losses totaled $5 billion, and 2019 projections have reached $19.5 billion. According to a 2016 Ponemon Institute Report, average demand is $2,500. Hackers responsible for the 2018 attack on the City of Atlanta, which destabilized city operations, demanded $50,000 in bitcoin. Ultimately, the city spent over $2.6 million to respond to the attack. Costs often incurred as a result of a ransomware event include loss of income, forensic investigation expenses, legal fees, data recovery and digital asset restoration costs. Given these potentially exorbitant costs, it is sometimes easier and cheaper to pay the ransom, which even the FBI acknowledges and often advises.

CYBER RISK

READY, SET, ACTION… IF DATA BREACH TRENDS WERE MOVIES

2019 DATA BREACH PREDICTIONS

- **Game of Hackers** – "The (Cyber) Winter is Coming." Exploits are becomingly increasingly complex and available; however, the skillset needed to use them continues to decrease. As the barrier to entry for hacking lowers and the criminal justice deterrent remains far behind, expect 2019 to be yet another year of voluminous and widespread breaches.
- **PolterHeist** – "They're heeeeeeere." Unless companies truly integrate cyber due diligence into M&A transactions, expect more SPG-Marriott like situations where companies make investments in already breached assets and pay the price months and years down the line.

- **The Wizard of Crypto** – "Toto, I've got a feeling we're not unhackable anymore." Expect more high profile cases of crypto theft through SIM swapping, exchange hacking and other new techniques under development against the supposedly "unhackable" blockchain-based technology. The next time someone tells you something is unhackable, ask them how many locks have ever been invented without a matching key?
- **Cyber Wars –** The Enterprise Strikes Back. "Hackers, we are your daddy." Expect more companies to switch focus from reactive, border defense, technology-based strategies to pre-emptive and dynamic security based on contextualized threat intelligence. Those who adapt will survive. Those who cling to a fortress mentality will starve during the siege.

2018 DATA BREACH TRENDS

- **Fight Club** – "The first rule of Fight Club is: You do not talk about Fight Club." Underground forums boost cyber-criminal effectiveness; dark web forums replete with hacker horse-trading of malware, rootkits, and "ransomware-as-a-service" which empower hacking forces and making for easy pay days.
- **The Godfather** – "I'm going to make him an offer he can't refuse." As the Corleon family was the last one standing after the Five Families War, Ransomware families declined in 2018, but demands more than doubled in value.

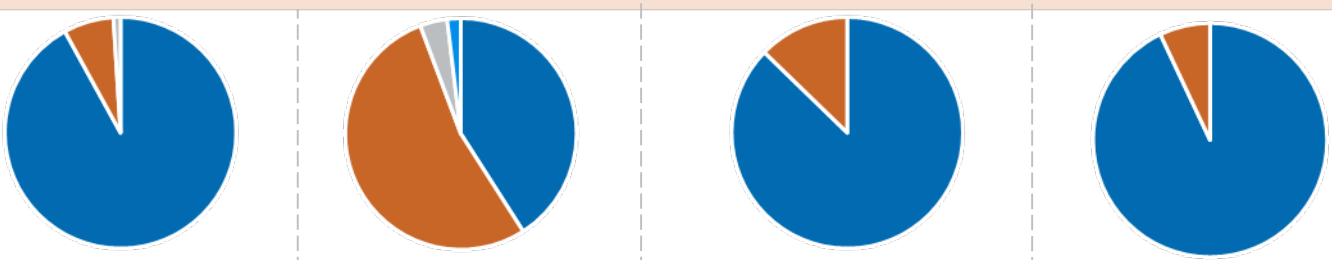
- **Clueless** – "Oh my gosh, I'm totally buggin'." Malvertising campaigns increase as hackers lure unsuspecting victims to landing pages with hidden exploits. Additionally, large scale credit card thefts have shifted from POS to e-commerce sites.
- **I, Robot** – Internet of Things (IoT) malware up 73% in the third quarter of 2018.
- **The Money Pit** – "Here lies Walter Fielding. He bought a house, and it killed him." Cryptocurrency mining takes off as hackers take advantage of lax security and use cameras and video recorders to create cryptomining supercomputers that suck power and computing resources from unknowing victims.
- **The Bank Job** – Financial Sector breaches increase 20% in 3Q18.

CYBER RISK

INDUSTRY 2018 BREACH STATISTICS

FINANCIAL	HEALTHCARE	MANUFACTURING	RETAIL
598 Incidents with 146 confirmed data disclosures	750 Incidents with 536 confirmed data disclosures	536 Incidents with 73 confirmed data disclosures	317 Incidents with 169 confirmed data disclosures

THREAT ACTORS — External, Internal, Partners, Multiple Parties



ACTOR MOTIVES — Financial, Espionage, Fun, Convenience

DATA COMPROMISED — Personal, Payment, Bank, Medical, Secrets, Credentials

SECOND HALF 2018 RENEWAL PURCHASING TRENDS

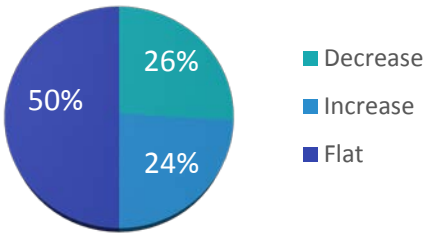
CHANGES IN PRIMARY PRICING

.89%

Average Change in Primary Pricing Per Million

Inclusive of all flat renewals but exclusive of changes of +/- 20%

PRIMARY RENEWALS PRICE PER MILLION



EMPLOYMENT PRACTICES

THE STATE OF THE EMPLOYMENT PRACTICES LIABILITY MARKET

The employment practices market continues to take a wait-and-see approach as the expected onslaught of claims emanating from the #metoo movement and equal pay discrimination has yet to take effect. Additionally, many experts wonder what impact the Supreme Court's action arbitration waiver ruling will have on the employment class action arena, specifically whether the demand for wage and hour coverage will decrease.

MANDATORY ARBITRATION: WIN FOR EMPLOYER. In May 2018, the Supreme Court ruled in a 5-4 decision *Epic Systems Corp. v. Lewis* that arbitration clauses in employment contracts are enforceable, thus requiring employees to resolve disputes individually and outside of court. The Supreme Court reviewed two laws: the Federal Arbitration Act of 1925, which favors arbitration, and the National Labor Relations Act of 1935, which upholds employees' right to take collective action. Seen by many as limiting employees' rights in bringing employment-related class actions, *Epic* is a significant victory for employers. Concerned that *Epic* will silence the #metoo movement and make wage claims impossible to pursue, Democrats proposed legislation to upend the decision. Titled Restoring Justice for Workers Act, it is unlikely the bill becomes law during President Trump's administration, but many expect the topic to come up during the next presidential race. In an effort to prevent any negative impacts on #metoo, a bipartisan group of congressional leaders introduced the Ending Forced Arbitration of Sexual Harassment Act, which would exempt sexual harassment cases from mandatory arbitration. All 50 state attorneys general have urged Congress to approve the bill.

FLYING SOLO? Where class certification is not an option, plaintiffs' firms with sufficient resources may be willing to individually arbitrate the related claims of a large number of claimants. Beginning in August 2018, 12,501 Uber drivers filed for arbitration alleging they were misclassified as independent contractors. Similarly, Chipotle currently has 2,814 pending arbitration claims. It is speculated that some of the attorneys behind the mass arbitration proceedings likely do not intend to arbitrate every claim but seek to leverage early results to settle the bulk of the claims. Consider Buffalo Wild Wings' decision to settle with a reported 391 wage and hour claims rather than pursuing arbitration. Some international companies are likewise experiencing the pitfalls of trying individual cases. For example, Wal-Mart subsidiary Asda is currently in tribunal in the UK with 15,000 former and current employees over equal pay claims. On January 31, 2019, an appeals court ruled that Asda store employees may compare their jobs with distribution center employees. At last report, defense expenses exceeded $50 million. Similar claims are pending against Tesco, Morrisons, and Sainsbury's. If the supermarkets lose, the total payout reportedly may exceed 10 billion.

EQUAL PAY. Throughout 2018, more and more states implemented equal pay legislation. While New York and California have led the way in condensing the gender pay gap, the latest states enacting legislation include Washington, New Jersey, Florida, and New Hampshire. Some of these laws require employers to justify any employee pay differences even where employees do not work at the same establishment and forbids employers from prohibiting employees from discussing wages. Citigroup has led the way and publicly reported its deficiencies between male and female pay, bridging the void where discrepancies are found. Other companies incorporating equal pay into corporate policies include Google, Amazon, and Costco. With large corporations publicly changing internal policies, there may be greater pressure on other businesses to follow suit and more discrimination claims against those who do not.

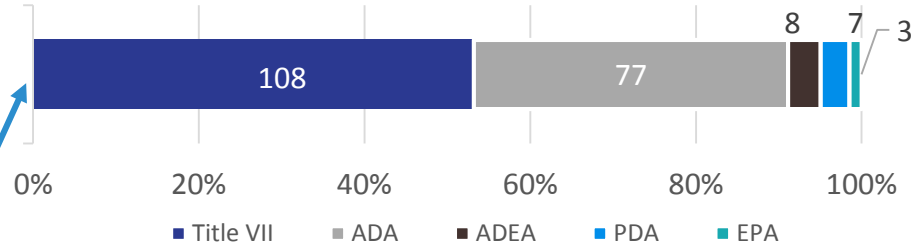
EMPLOYMENT PRACTICES

EEOC SNAPSHOT

Year	# of Charges	# of EEOC Initiated Lawsuits
2014	88,778	133
2015	89,385	142
2016	91,503	86
2017	84,254	184
2018	76,418	199

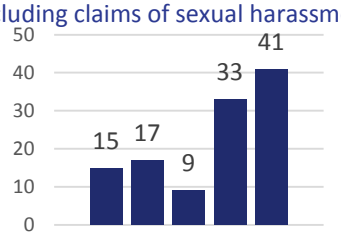
The Senate has not voted on President Trump's nominees for the Chair, two Commissioners, and the General Counsel. Once the positions are filled, many expect the number of filings to fall. Although the filings have increased in 2018, the top 10 government settlement amounts decreased, dropping from $485.25 million in 2017 to $126.7 million in 2018.

2018 FILINGS BY STATUTE



#METOO EFFECT

Title VII sexual discrimination filings including claims of sexual harassment



EEOC YE 2018 HIGHLIGHTS

- EEOC has shifted focus to larger, systemic cases. Filings may be down, but lawsuits are up.
- 74% of 2018 filings alleged sex-based discrimination vs. 65% in 2017.
- 11 Equal Pay Act lawsuits were filed in 2018 as compared to 6, 5, and 2 in 2016, 2015, and 2014, respectively.
- Total Monetary Relief: $505 million in total relief (litigation, mediations, and pre-litigation investigations) vs. $484 million in 2017.

LGBT PROTECTED UNDER TITLE VII? The EEOC has continually maintained that discrimination based on sexual orientation or gender identity is prohibited under Title VII. However, the Department of Justice under President Trump's administration disagrees, arguing Title VII does not cover LGBT discrimination. Despite this stance, plaintiffs and the EEOC continue to win cases with victories in the Second and Seventh Circuits, joining numerous district and administrative courts in the country that find Title VII extends to LGBT discrimination. The differing views among agencies and in the courts make many experts believe the Supreme Court will take an LGBT case in the near future.

ADA WEBSITE ACCESSIBILITY. Following Gil v. Winn-Dixie Stores, Inc., employers should consider whether their websites are accessible under Title III of the ADA, as websites may be considered "public accommodations." To help employers address website accessibility, the ADA has compiled a 27 item checklist. Considerations include text descriptions for links and navigation menus, HTML alt tags for images for hearing-impaired visitors, and corresponding audio descriptions for the visually impaired.

SECOND HALF 2018 RENEWAL PURCHASING TRENDS

(Based on McGriff FSD public company 2H 2018 renewals)

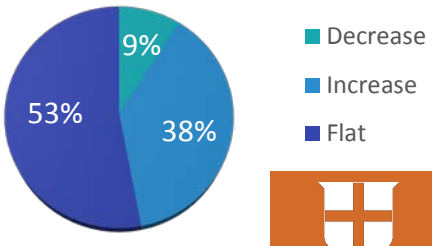
CHANGES IN PRIMARY PRICING

1.79%

Average Change in Primary Pricing Per Million

Inclusive of all flat renewals but exclusive of changes of +/- 20%

PRIMARY RENEWALS PRICE PER MILLION



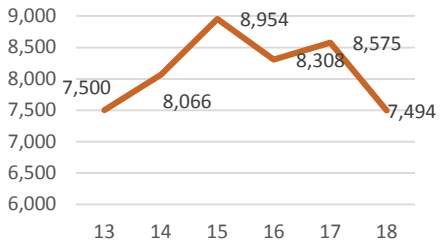
EMPLOYMENT PRACTICES

FLSA LITIGATION LANDSCAPE

FLSA

Fair Labor Standards Act of 1938 establishes standards for minimum wage, overtime, hours worked, recordkeeping and child labor.

FLSA CASES FILED IN FEDERAL COURT



COMMON ALLEGATIONS

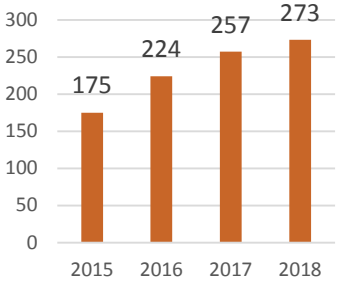
Overtime
Off-the-clock
Misclassification
Missed Meals & Breaks
Minimum Wage
Donning & Doffing
Tip Pooling

TOP INDUSTRIES

Retail
Financial Services / Insurance
Healthcare
Food & Food Services
Transportation / Shipping
Technology
Telecommunications / Utilities
Manufacturing

FLSA CLASS CERT RULINGS INCREASE WHILE DECERTIFICATION DECREASE

FLSA class certification rulings



FLSA conditional class certification results

79%

Success rate for plaintiffs in 2018 vs 73% success rate in 2017

FLSA Decertification Rulings

52%

Success rate for defendants in 2018 vs 63% success rate in 2017

WHY WAGE & HOUR LITIGATION IS LIKELY TO CONTINUE

- Significant migration of plaintiffs' attorneys to Wage & Hour litigation
- Low cost investment by the plaintiffs' bar. Plaintiffs do not need an expert witness and do not have to conduct significant discovery in seeking class certification.
- Minimum wage hikes in 21 states and 22 major cities took effect in 2017.
- Technology and social media allow for more cost-effective advertisement of cases by plaintiffs' bar.
- Most often, defendants are not 100% compliant with Wage & Hour laws.

TOP SETTLEMENTS OF 2018

TOP 10 **PRIVATE PLAINTIFF WAGE & HOUR** CLASS ACTION SETTLEMENTS

1. $65M – Wal-Mart Stores, Inc.
2. $54.5M – Bloomberg L.P.
3. $27.5M – Wells Fargo
4. $25M – Abercrombie & Fitch Co.
5. $19.1M – Carlson Restaurants, Inc
6. $16.8M – Kellogg Company
7. $15M – J.B. Hunt Transport, Inc.
8. $11M – Bank of America, N.A.
9. $10M – CBS Television Studios
10. $9.6M – Abercrombie & Fitch Trading Co.

TOP 10 **PRIVATE PLAINTIFF EMPLOYMENT DISCRIMINATION** CLASS ACTION SETTLEMENTS

1. $90M – Twenty-First Century Fox, Inc.
2. $45M- Family Dollar Stores
3. $24M – JP Morgan Chase Bank
4. $22.5M – Nucor Corp.
5. $10M – Twenty-First Century Fox, Inc.
6. $10M – Uber Technologies, Inc.
7. $4M – Forest Laboratories, Inc.
8. $3.75M – Koch Foods of Mississippi LLC
9. $3.74M – Target Corp.
10. $3.1M – Chadbourne & Parke

TOP 5 **GOVERNMENT INITIATED MONETARY SETTLEMENTS**

1. $47M – Credit Suisse Group AG – Asia hiring practices
2. $20.8M – The City of New York– gender discrimination
3. $16M – First Farmers Financial – ERISA violations on investment misrepresentation
4. $13.9M – Imperial Pacific International – Wage Hour Violations
5. $5.5M – Waste Management, Inc. – Undocumented workers

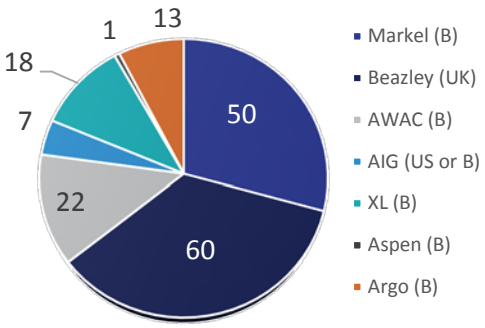
EMPLOYMENT PRACTICES

WAGE & HOUR UPDATE

INSURANCE SOLUTIONS. Due to underwriting difficulties and insurability concerns (except defense costs), Wage & Hour / FLSA violations have historically been excluded under employment practices insurance policies (EPL). In 2013, Bermuda and London markets began offering Wage & Hour coverage (separate from EPL) at high retentions ($5 million or more). In 2015, Beazley began offering an alternative product targeted for companies with 1,000 to 10,000 employees at lower retentions. Increased competition, primarily in Bermuda and London, has led to more competitive premiums and retentions and an increasing number of companies purchasing Wage & Hour insurance. The graphic below provides greater detail regarding product development.

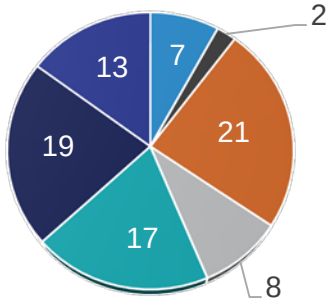
PRIOR TO 2012	2012 & 2013	2014	2015	2016 & 2017	2018
# of policies: **0**	# of policies: **5-7**	# of policies: **10**	# of policies: **45**	# of policies: **90** to **126**	# of policies: **171**
W&H claims were excluded under all EPL policies. A few insurers would offer a defense-cost-only extension with a sublimit of $150,000 to $250,000 excess of the EPL retention.	The Bermuda market (Markel, AWAC and XL) introduced separate W&H defense and indemnity coverage with a minimum $5 million retention and 15% to 20% coinsurance at $25,000+ per million. The product was geared toward very large employers willing to assume higher retentions.	The Bermuda market began to offer combined W&H/EPL policies via endorsement offering shared limits and a credit.	In October 2015, Beazley London introduced an EPL / W&H product, available as a combined or separate product. The target market was 1,000 to 10,000 employees with retentions of $500,000 ($250,000 for some risks).	Aspen Bermuda entered the market. Beazley London continued to be the most aggressive with retentions, quoting as low as $100,000 but also trying to keep retentions 10% of limit. Argo Bermuda entered in 2017 with the same approach as Beazley London.	Total number of W&H placements in the market as of year end 2018 increased from 88 in 2016 to 126 in 2017 to 171 in 2018.

OF PRIMARY POLICIES

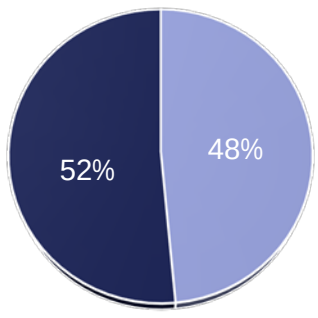


Total Buyers: 171

OF EXCESS POLICIES



STAND-ALONE VS. BLENDED



FIDUCIARY LIABILITY

The Fiduciary Liability market remains stable as premiums have reached what most consider minimums and coverage continues to expand. Many carriers are interested in growing their Fiduciary Liability book of business; however, current pricing is preventing new carriers from winning based on premium alone. Retentions are decreasing due to market competition and the reduction of company stock as a percentage of total plan assets. As a way to differentiate themselves, several carriers will waive renewal application requirements in offers of two year policies or guaranteed renewals. In contrast, excessive fee litigation has prompted other carriers to require supplemental applications or otherwise give additional underwriting scrutiny to insureds' investment manager selection practices.

DO FIDUCIARY DUTIES APPLY TO CYBERSECURITY? While ERISA requires fiduciaries of employee benefit plans to act in the best interests of the plan participants, it does not explicitly state that fiduciaries are responsible for plan participants' personally identifiable information (PII). Likewise, HIPAA imposes rules for safeguarding protected health information (PHI), but it does not protect PII in retirement, pension, or welfare benefit plans. Given the increasing number of cyber breaches, coupled with heightened regulatory focus on information protection, many expect plan participants to claim that cybersecurity is an obligation of fiduciaries managing employee benefit plans. The Anthem breach, which affected nearly 79 million individuals and resulted in a $115 million settlement in 2017, is expected to pave the road for future litigation.

COULD STOCK DROP CLAIMS MAKE A COMEBACK? Since the Supreme Court's decision in *Fifth Third Bank Corp. v. Dudenhoeffer* created a new (and tougher) standard in breach of prudence claims involving non-public information, many thought stock drop claims would go the way of the Dodo bird. However, the recent Second Circuit decision in *Jander v. Retirement Plans Committee of IBM* may make stock drop claims cool again. In this case, investors in the IBM Company Stock Fund alleged that plan fiduciaries violated their duty of prudence by allowing the continued investment in IBM common stock despite knowing a division of the company was losing money. Ultimately, IBM announced that its microelectronics business lost $700 million, and IBM's stock fell by $12 a share. Although the district court dismissed the case based on the *Dudenhoeffer* standards, the Second Circuit reversed, finding that no prudent fiduciary could conclude that an earlier corrective disclosure of the microelectronics business' impairment would have caused more harm than good to the ESOP. The Second Circuit's decision stands out as departing from Dudenhoeffer's theory that disclosure of inside information could do more harm than good to stock held in the plan.

THE PROBLEM WITH KEEPING IT IN THE FAMILY. If you have a good product, you want your employees to use it, too, right? Sure, but you may find yourself in trouble if your employees pay more than the product's commercial price. Financial services companies continue to find themselves embroiled in ERISA litigation concerning employee retirement plan investments in proprietary in-house funds where nearly identical, lower cost versions of the same funds are available to commercial customers. Despite ERISA's proprietary fund exemption, the same fiduciary standard applies. Thus far, the plaintiffs' bar has been successful in claiming conflicts of interest in these cases, and many claims have resulted in DOJ investigations.

FIDUCIARY LIABILITY

FEE CASES CONTINUE. Following the Supreme Court's decision in *Tibble v. Edison*, which held that plan fiduciaries have a continuing duty to monitor trust investments and fees associated with the plan's investment alternatives, excessive fee litigation continues. Plaintiffs typically allege plan fiduciaries breached their duties by failing to identify excessive administrative and management fees paid to administrators of a plan. Plaintiffs further allege that such fees are misleading and must be disclosed. In addition to 401(K) fees being questioned, university plans, or 403(B) plans, have also undergone scrutiny for excessive fees. A list of all defendants who have settled excessive fee cases follows.

- Allianz
- Allina Health Systems
- American Airlines
- American Century
- Anthem, Inc.
- AT&T
- Banner Health
- BB&T
- Blackrock
- Board of Trustees of Supplemental Income Trust Fund
- Brown University
- Capital Group Companies, Inc.
- Charles Schwab
- Checksmart
- Chevron Corp.
- City National
- Columbia University
- Cornell University
- CVS
- Delta Airlines
- Deutsche Bank Americas
- DST Systems
- Duke University
- Edward Jones
- Emory University
- Essentia Health
- Fidelity
- FirstGroup America, Inc.
- Franklin Templeton
- Fujitsu
- General Electric
- Georgetown University
- Great-West
- Gucci America, Inc./Kering Americas
- Home Depot
- HP
- Huntington Bancshares
- Insperity
- Intel
- Invesco
- Jackson National
- Johns Hopkins
- Kaleida Health
- LaMettry
- Lowe's Companies, Inc.
- M&T Bank
- Morgan Stanley
- Mutual of Omaha
- Neuberger Berman
- New York Life Insurance
- Nordstrom, Inc.
- Northrop Grumman
- Northwestern University
- Norton Healthcare Inc.
- Novitex Enterprise Solutions, Inc.
- Oracle
- Pioneer Natural Resources
- Princeton University
- Principal Life Insurance
- Putnam Investments
- Safeway
- SEI Investments Co.
- Starwood Hotels & Resorts
- T. Rowe Price Group
- TIAA-CREF
- Transamerica (Aegon)
- United Airlines
- University of Chicago
- University of Pennsylvania
- University of Rochester
- University of Southern California
- Vanderbilt University
- Verizon Communications
- Voya
- Waddell & Reed Financial Inc.
- Wal-Mart
- Washington University
- Wells Fargo
- Yale University

SECOND HALF 2018 RENEWAL PURCHASING TRENDS

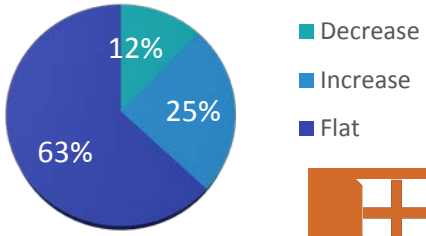
CHANGES IN PRIMARY PRICING

1.15%

Average Change in Primary Pricing Per Million

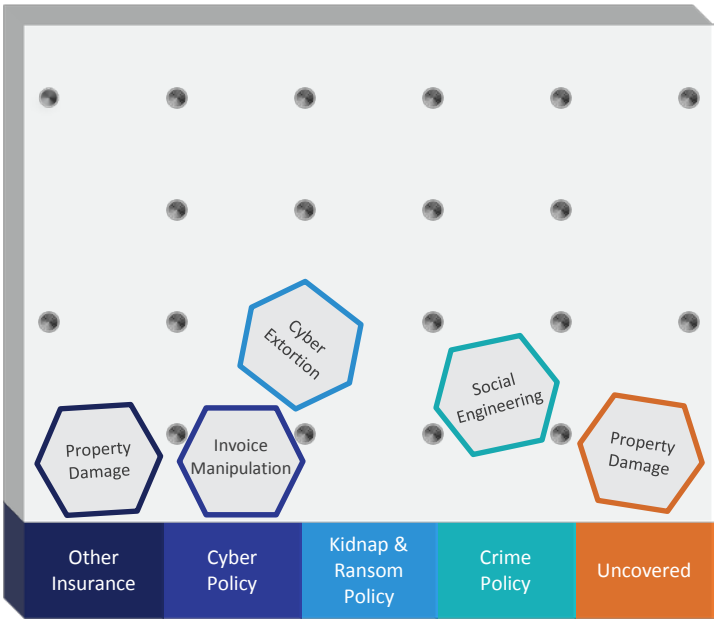
Inclusive of all flat renewals but exclusive of changes of +/- 20%

PRIMARY RENEWALS PRICE PER MILLION



COMMERCIAL CRIME

SOCIAL ENGINEERING PLINKO™



Loss of money and property, extortion demands, loss of data and goodwill. All companies are at risk of losing significant assets as a result of social engineering schemes. The means by which a fraudster enters a system and what the fraudster intends to steal continues to evolve, creating confusion regarding which policies cover the various losses.

The original social engineering scheme to which many companies have fallen prey is fraudulent impersonation, or "Fake President" emails. In this scheme, the fraudster impersonates a high level executive and asks the targeted employee to wire an amount of money to a specific account within a small timeframe.

Initially, all losses resulting from such schemes were submitted under Computer Fraud insuring agreements of Commercial Crime policies. Although insurers challenged the applicability of Computer Fraud to these losses, insureds generally prevailed. In response, carriers amended their policies to provide sublimited coverage for social engineering loss.

Attempting to curtail losses, many companies have adopted payment authority controls, including dual authentication and call back provisions confirming new payment instructions. But as fraudsters become increasingly sophisticated, losses continue.

In addition to fraudulent impersonation, fraudster's engage in invoice manipulation schemes whereby payment instructions on legitimate vendor invoices are changed to direct payment to the fraudster account. In such a scheme, both the client and the vendor are harmed – the vendor does not receive payment, and the client still owes payment. Without social engineering coverage, the loss of funds may not be covered under a commercial crime policy. Thus, many cyber policies now cover the inability to collect on an invoice as a result of a breach.

If a social engineering scheme results in a loss that is not covered under any policy, the overall client relationship could be at stake, posing a larger threat to companies everywhere. The following pages provide case summaries involving what seems like a game of social engineering Plinko™.

COMMERCIAL CRIME

SCOREBOARD: OVERVIEW OF CIRCUIT COURT RULINGS ON SOCIAL ENGINEERING COVERAGE

CIRCUIT COURT AND CASE	INSURED	CARRIER
5th Circuit: *Apache v. Great American*		X
2nd Circuit: *Medidata v. Chubb*	X	
6th Circuit: *American Tooling Center v. Travelers*	X	
11th Circuit: *Ironshore Indemnity v. Principle Solutions*	PENDING	
9th Circuit: *Aqua Star (USA) Corp. v. Travelers*		X

COVERAGE TWICE AFFIRMED UNDER INSUREDS COMPUTER FRAUD INSURING AGREEMENT

In July 2018, two federal appeals courts confirmed coverage for social engineering losses under the Computer Fraud insuring agreements of the insureds' commercial crime policies. On July 6th, the Second Circuit affirmed the district court's ruling that Medidata's Commercial Crime policy provides coverage under the policy's Computer Fraud Insuring Agreement for the $4.8 million wire transfer sent by Medidata to a fraudulent account as a result of an email spoofing scheme. The loss was initiated in 2014 when fraudsters achieved entry into Medidata's email system and copied a computer code allowing the email format to mimic internal emails while disguising the fraudster's identity. The $4.8 million request purportedly sent by the CEO to the accounting employee was granted despite the approval of senior level officers and payment verification. After an appeal by Chubb, the Second Circuit affirmed the district court's ruling by asserting that the company's email system falls within the definition of Computer System under the policy and the direct loss was as a result of the spoofed emails. On July 13th, the Sixth circuit reversed a lower court's decision and ruled Travelers must cover the $834,000 loss experienced by American Tooling Center as a result of fraudsters impersonating employees of a vendor in a series of emails.

In addition to the Second and Sixth Circuit rulings, several cybercrime coverage cases have worked their way through other appellate courts. We are starting to see new case law in the area of cybercrime coverage as the various appellate courts interpret the Computer Fraud insuring agreements of crime policies. A more in-depth summary for each case follows.

FIFTH CIRCUIT

Apache Corporation v. Great American Insurance Company — An accounts payable employee of Apache received a call from an imposter claiming to be an employee of Apache vendor Petrofac Facilities Management Ltd. The imposter told the employee that Petrofac had a new bank, Royal Bank of Scotland, where future wire payments should be sent. The employee requested an email with a written request on Petrofac letterhead. Upon receiving the written request, the Apache employee called the telephone number on the letterhead to verify the request but, unbeknownst to the employee, spoke to an imposter. After a second Apache employee approved the request, Apache sent $7 million to a fraudulent account before the fraud was discovered. Apache was able to recover $2.4 million of the stolen money and filed a claim with Great American for the remainder. Great American denied coverage under the crime policy's Computer Fraud insuring agreement. Apache sued and the district court granted summary judgment in favor of Apache. Great American appealed to the Fifth Circuit, and the court held the loss was not covered under the policy's computer fraud provision.

COMMERCIAL CRIME

NINTH CIRCUIT

Aqua Star (USA) Corp. v. Travelers Casualty and Surety Company of America — Aqua Star vendor Zhanjiang Long Wei Aquatic Products Industry Co., based in China, was hacked. After intercepting emails between both parties, the hackers gained control over the email system and sent Aqua Star an email providing fraudulent bank account information for the vendor. Aqua Star's employees made the change, and the company transferred $700,000 to the fraudulent account before the loss was discovered. Aqua Star filed a claim under its Travelers crime policy. Travelers denied the claim under the Computer Fraud coverage. Aqua Star filed suit, and the district court granted summary judgment in favor of Travelers. Aqua Star appealed to the Ninth Circuit. Applying Washington law, the court affirmed the summary judgment.

Ubiquiti Networks, Inc. v. National Union Fire Insurance Co. (AIG) — Although this is not an appellate case, it is a case pending in the Superior Court of the State of California, which is in the Ninth Circuit. Ubiquiti's Chief Accounting Officer received an email purportedly from Ubiquiti's CEO with a request for a funds transfer to a foreign bank account. Additionally, Ubiquiti's true CEO received phone calls from an imposter posing as Ubiquiti's mergers and acquisitions attorney. Before discovering the fraud, Ubiquiti transferred $46,683,232 to the foreign account. Ubiquiti recovered $16,378,401 and filed a claim under its AIG crime policy for the remainder. AIG denied the claim finding that Computer Fraud coverage applies only where a fraudulent transfer results from the direct hacking of an insureds computer system.

ELEVENTH CIRCUIT

Principle Solutions Group LLC v. Ironshore Indemnity Inc.— A fraudulent email sent from a purported managing director of Principle to Principle's controller instructed the controller to wire $1.7 million for a company acquisition to an attorney working on the transaction. The email appeared to be sent from the corporate email address. The controller then received an email from the attorney who represented himself as a partner at Alston Bird and subsequently received a call from the attorney providing wiring instructions. The controller approved the wire transfer and even verified the instruction with the financial institution's fraud prevention unit. The fraud was discovered, and a claim was made under the Computer and Funds Transfer Fraud section of Ironshore's crime policy. Ironshore denied the claim stating the initial email did not include instructions for transferring the funds, and several acts occurred before the transfer of funds. Principle filed suit in federal court in Georgia. The district court judge found the policy language for the Computer and Funds Transfer Fraud coverage to be ambiguous and ruled in favor of Principle. Ironshore has appealed the ruling to the Eleventh Circuit.

SECOND HALF 2018 RENEWAL PURCHASING TRENDS

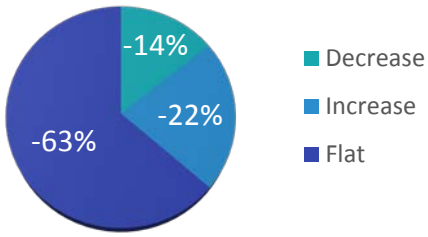
CHANGES IN PRIMARY PRICING

-0.4%

Average Change in Primary Pricing Per Million

Inclusive of all flat renewals but exclusive of changes of +/- 20%

PRIMARY RENEWALS PRICE PER MILLION



CLIENT FOCUSED, RESULTS DRIVEN

McGRIFF, SEIBELS & WILLIAMS, INC.

3400 Overton Park Drive SE | Suite 300 | Atlanta, GA 30339
(800) 476-2541 | (404) 497-7500 | **www.mcgriff.com**