SUMMER 2018

Perspectives on Insurance Recovery

pillsbury

Expanding the Boundaries of Coverage in the Face of Evolving Risks

Advances in technology, social change, new regulations—developments like these challenge companies' risk-mitigation efforts and insurance programs. As the articles in this newsletter illustrate, Pillsbury's Insurance Recovery & Advisory group provides guidance at the forefront of emerging risks. How does insurance apply to acts by artificial intelligence? Are smart contracts smart enough to work in the insurance industry? How can existing insurance policies—and new ones—be wielded to limit the losses from cybersecurity breaches? Implementation of the EU's General Data Protection Regulation (GDPR) and enhanced awareness brought about by the #MeToo movement may require re-evaluation and modification of policies and coverages. Pillsbury's IRA Group also continues to push the boundaries of insurance recovery issues, such as identifying D&O insurance coverage for statutory appraisal proceedings and strategies for maximizing available insurance coverage for sublimited losses. In the following pages, we tackle these topics and more, with additional insights available on our blog (**PolicyholderPulse.com**), and Twitter (**@PHPulseLaw**).

Table of Contents

By Peri N. Mahaley

Everybody knew it was coming. But many companies are still scrambling to figure out how the EU's General Data Protection Regulation (GDPR)—which went into effect on May 25, 2018—will affect how they do business. But while publications are awash with advice regarding compliance, few tackle the question whether your business is protected against loss in the event of a data breach or other unintentional failure to comply. We strongly suggest that your due diligence include a review of your insurance coverage for GDPR non-compliance, especially for fines, penalties and lawsuits (individual or class action).

Coverage for Costs of Compliance

Many costs that companies will incur to comply with GDPR simply will not be covered by any insurance. Insurance is designed to respond to fortuitous loss or liability, not ordinary costs of doing business. Thus, for example, coverage likely is unavailable for expenses to implement data security measures, maintain required records or hire a Data Protection Officer.

On the other hand, the cost of notification in the event of a data breach is a standard feature of specialized "cyber" insurance policies. The GDPR requires a "controller" of personal data to notify the relevant supervisory authority "without undue delay" and, where feasible, within 72 hours of discovering a breach, unless the breach is unlikely to involve a "risk to the rights and freedoms of natural persons."

Further, where the breach is likely to result in a high risk to such rights and freedoms, the controller also must notify the affected data subjects without undue delay, subject to certain exceptions. Cyber policies generally do cover the cost of notification to individuals. You should examine your policy to make sure that coverage applies in the event of a suspected breach as well as in the case of known unauthorized disclosure. On the other hand, not all cyber policies currently cover the cost of notifying privacy regulators—an important coverage addition to explore with your insurer at renewal time.

In addition, cyber policies typically cover fees for legal advice on compliance with breach notification laws. A best practice would be to expressly include GDPR among the "Privacy Laws" enumerated in your cyber policy.

Coverage for Fines and Penalties

Commentators have expressed doubt whether coverage will be available for GDPR fines, in part because of their sheer magnitude. The GDPR provides for two tiers of administrative fines—the higher topping out at the greater of a whopping €20 million or 4% of global annual turnover for the preceding financial year. The higher tier applies to a wide range of violations, including processing personal data without either the subject's express consent or one of several prescribed alternative justifications; failure to provide data subjects with transparent information regarding their rights under the GDPR; failure to give the data subject required access to his or her data or to rectify inaccurate data; and failure to comply with the rules governing the transfer of personal data outside the EU. Lower-tier fines—up to the greater of €10 million or 2% of global annual turnover for the preceding year—apply to violations such as failure to timely notify the supervisory authority of a breach, to cooperate with the data protection supervisory authority, or to appoint a Data Protection Officer.

Cyber policies generally do provide coverage for civil fines and penalties imposed by governmental authorities for breach of privacy laws, but there are three key caveats in relation to GDPR. First, many cyber policies today limit coverage for regulatory fines and penalties to those imposed as the result of a data breach. Fines imposed for violations of non-breach-related GDPR provisions may not be covered under such policies. A second real concern is whether it will even be possible to obtain full protection. Analysts have noted that, based on its revenues, a typical FTSE 100 company could face up to £5 billion for GDPR violations. Very large companies may be able to purchase over $100 million in cyber coverage, but probably nowhere near the theoretical maximum of a GDPR fine. Finally, cyber policies commonly contain language barring coverage for fines and penalties unless they are "insurable by law." The better policies also provide that the insurability of fines or penalties shall be determined by the "laws of any applicable jurisdiction that most favors coverage for such monetary fines or penalties." Uncertainty nevertheless arises because the insurability of fines such as those imposed by the GDPR largely has not been tested in EU courts (or U.S. courts, for that matter), while several European jurisdictions appear expressly to prohibit insurance for such penalties. For these reasons, policyholders and insurers alike should consider enhancement of current policy wordings and limits in light of GDPR.

Also importantly, only civil fines are covered by insurance—criminal penalties almost never are. GDPR administrative fines are civil in nature. But the GDPR permits EU Member States to impose their own penalties for violations outside of administrative fines. These penalties may be criminal in nature and most likely would not be covered.

Coverage for Third-Party Liability

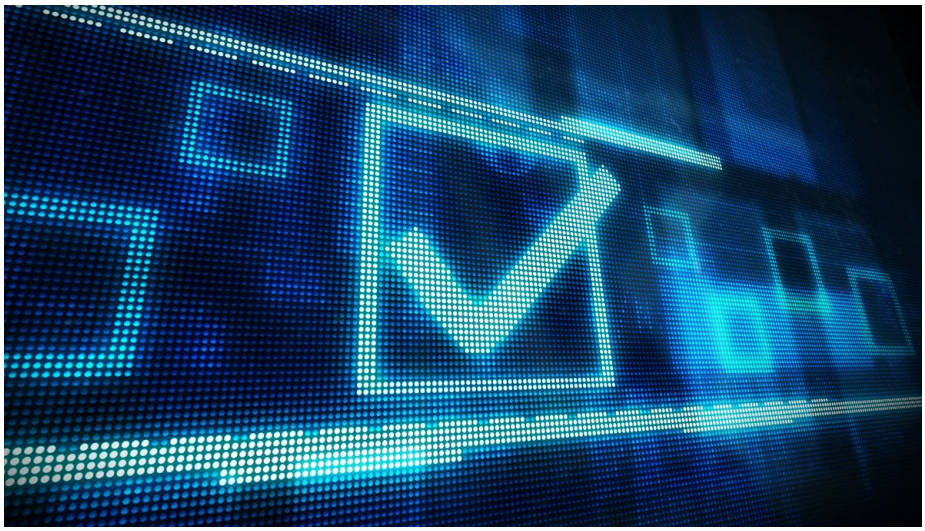
The GDPR also confers a private right of action on data subjects for violations of the regulation. Individuals may seek monetary damages in the EU Member State in which they reside, or in which the defendant data controller or processer has an establishment. Although cyber policies provide coverage for damages and defense costs arising out of third-party claims due to privacy breaches, not all claims for violations of GDPR would be covered under many current wordings. Some policies cover liability arising out of the unauthorized access to or disclosure of personally identifiable information, but do not address the wrongful collection or processing of information in the absence of disclosure, the failure to provide individuals access to their own information or to correct or delete data when requested, or the failure to make required disclosures when obtaining data subjects' consent.

Just the Beginning

Many see the GDPR as only the first of such laws to be passed. The California Consumer Privacy Act of 2018 was passed in record time and signed into law June 28, 2018, to go into effect January 1, 2020. The CCPA has many features that are similar to the GDPR, including a focus on consumers' rights to obtain information about how their information is being collected and for what purpose, to request deletion of their information, and to opt out of the sale of their information. Other states are expected to follow suit.

Cyber policies remain a vital source of protection for businesses soon to be subject to the GDPR and U.S. state laws. But policyholders need to re-evaluate their programs, and insurers need to continue to modify policies to maintain competitive value. Ready or not, the GDPR and its progeny are here to stay.

Peri N. Mahaley is senior counsel in Pillsbury's Washington, DC, office.



Are Smart Contracts Smart Enough for the Insurance Industry?

By Kimberly Buffington and Cara Adams

Third-party intervention may now prove unnecessary when interpreting and enforcing contract provisions—at least this is what proponents of smart contracts believe. The overall goal, they argue, is to provide security unattainable through traditional contract law and to reduce additional transaction costs that come with the traditional process. Will insurance policies become the laboratory to test their thesis?

First imagined by computer scientist Nick Szabo in 1996, smart contracts are computer protocols meant to facilitate a contract's implementation and performance. They can carry out only the specific instructions given to them, and all transactions are traceable and irreversible. Regarding functionality, experts have likened smart contracts to a vending machine; contract terms are first coded and placed within the block of a blockchain (the same technology Bitcoin uses). Once the triggering event occurs, the contract is performed consistent with all designated terms. Continuing the analogy, the individual inserting money in the vending machine sets off a chain of events, unable to be undone or halted midway. (Granted, this last part isn't like the traditional vending machines we know.) The machine keeps the money and dispenses the item. The contract has been fully performed.

Insurance Agreements

Whether there is room for smart contracts in the insurance context remains to be seen. Generally, the "if this occurs, then that" nature of insurance policies lends itself to the conditional nature of smart contracts. In June 2017, AIG announced a partnership with IBM to develop a "smart insurance policy" for international markets. It will be interesting to follow this arrangement to see how well smart contracts can function in the insurance space. Smart contracts have the potential to play a helpful role in a variety of aspects within the industry. They could allow policy documents to be stored on numerous ledgers simultaneously, so that they are available for simultaneous review and amendment by multiple parties, and can never be lost or changed without the parties' agreement. They may help secure policy documents and improve the claims process. They could remove administrative barriers and red tape throughout the system.

Further, smart contracts may affect the automated claims payment process. With smart contracts, policyholders could receive payments for uncontested claims immediately, instead of a month or more later, as under the current procedure. And the payouts could be sent directly to a customer's account. Smart contract supporters ultimately hope the claims management process can be smoothed and predetermined by algorithms within a code. Such a development would likely enhance customer satisfaction and might ultimately lower insurer costs, with the potential to reduce premiums.

Natural disasters such as floods, tornadoes or earthquakes could constitute triggering events that give rise to payouts automatically. The contract might even be programmed to ascertain the physical scope of the event, which in turn could ease the adjustment process by cutting down time spent investigating and verifying the claim. Insurers could program smart contracts to decrease the potential for fraud. An insurer could program a payment to occur only when the policyholder uses a provider of its choosing, for instance, and can further program the money to automatically return if the insured does not abide by the terms of the agreement. The process could become more transparent.

Potential Drawbacks

Of course, smart contracts have their flaws. First, some proponents suggest that smart contracts may also help avoid ambiguities in policy language, thus preventing disputes and lawsuits over ambiguous policy terms. But it would be unrealistic to expect smart contracts to eliminate ambiguities and resulting disputes any more than such disputes are currently eliminated by traditionally written contracts. Before considering using smart contracts, policyholders would be advised to carefully review the

proposed coverage terms and availability of recourse in the event of any issues.

Second, smart contracts must be coded by a third-party programmer, who must have the specialized knowledge necessary to design a contract that works well. Requiring a third party to program a smart contract touted for having the benefit of less involvement from outside professionals defeats one of the advantages of smart contracts.

Third, it highlights another potential problem: human error. The **hacking of The DAO,** a "decentralized autonomous organization" for venture capital funding, serves as the most well-known case involving coding gone wrong, with nearly $60 million dollars' worth of digital currency being compromised due to unaddressed security vulnerabilities. Not to mention the human input error that can arise in defining the scope of insurance coverage, such as covered entities, properties and values. Last, the insurance market is highly regulated, whereas smart contracts are not. Thus, smart insurance contracts may not be able to operate as smoothly in the insurance context as many anticipate.

Conclusion

As we head towards a landscape increasingly cluttered with advanced technology, it seems smart contracts have potential. Insurance management could definitely stand to be improved, and this may be one of the ways to push that process forward.

Kimberly Buffington is the office managing partner in Pillsbury's Los Angeles office.

Cara Adams is an associate in Pillsbury's Los Angeles office.

Your Broker May Be Wrong: Why Your D&O Policies Should Cover Delaware Appraisal Proceedings

By Peter M. Gillon and Benjamin D. Tievsky

It's now accepted wisdom that virtually all public company mergers and acquisitions will be challenged with at least one lawsuit—over 95% of them are. A less well-publicized form of challenge—and one that is both fascinating and perplexing for those interested in securities litigation—is the unique creature of Delaware law known as the appraisal proceeding. Under ***Delaware General Corporation Law §262****, shareholders dissenting from a merger on grounds that the share price they'll receive is inadequate "shall be entitled to an appraisal by the Court of Chancery of the fair value of the stockholder's shares of stock." If the court finds that the deal price is lower than fair market value, the acquiring corporation must pay the difference to the dissenting shareholders, plus interest. The court may also award their attorneys' and experts' fees, which can be significant. This process has created a cottage industry of "appraisal arbitrage," in which hedge funds purchase shares in hopes of securing a higher price for those shares through appraisal. Fortunately, D&O insurance might be available to cover the acquired company's defense and other costs.*

An insurance company's duty is to pay defense costs under D&O insurance is generally triggered by allegations of "Wrongful Acts" committed by the insured individual directors and officers or the company. Because a typical appraisal petition alleges the per-share acquisition price of the target company's stock and other basic facts relating to the merger, many in the D&O insurance "community" have viewed appraisal proceedings incorrectly as a simple exercise in economics, not an allegation of "Wrongful Acts."

This cramped approach ignores the reality of appraisal proceedings today, which tend to focus on the adequacy of the process by which the purchase price was determined. A board may have fulfilled its fiduciary duties but still have failed to meet the requirements of a fair process implicit in Section 262. Numerous recent decisions make this point. As the Chancery Court said in **In re: Appraisal of Dell Inc.**: "[A] sale process might pass muster for the purposes of a breach of fiduciary claim and yet still generate a sub-optimal process for purposes of an appraisal." In reviewing this process, the Chancery Court **may examine** whether there was meaningful competition among bidders, whether the seller offered adequate and reliable information, whether there was evidence of collusion or favoritism towards certain bidders, whether the seller sought topping bids during a go-shop period, and whether the board obtained an independent third-party valuation, among other factors.

While the claimant's burden of proof in establishing liability under Section 262 is relatively low, so is the standard for meeting the typical D&O policy's

requirement of an alleged "Wrongful Act." The definition of "Wrongful Act" commonly encompasses "any actual or alleged breach of duty, neglect, error, misstatement, misleading statement, [or] omission"—in short, almost any corporate act or omission. As a result, a board's alleged "omission" in failing to follow an adequate sales process may be considered a Wrongful Act under a D&O policy's broad definition of that term.

In many cases, the claimants may **couple their appraisal claim with a breach of fiduciary duty claim**, asserting improper self-dealing or other misconduct by a target company's directors and officers. Such allegations are well within the scope of the Chancery Court's Section 262 mandate, which is to consider "all relevant factors" in reviewing the sale process and determining the "true" pre-merger value of the company. Appraisal proceedings may also give rise to **separate breach of fiduciary duty and/or securities litigation**. The fact that appraisal proceedings generally delve into the adequacy of the sales process and other "relevant factors" provides a strong basis for coverage under D&O policies.

Another nuance to the trigger of coverage issue is whether an appraisal action is considered a claim against a board of directors or a claim against the corporate entity. As noted, inherent in appraisal proceedings today are implicit allegations of Wrongful Acts committed by the company's board. Allegations against individual directors and officers for Wrongful Acts typically trigger "Side B" coverage—D&O coverage for amounts that the company must pay to indemnify those individuals. The named defendant in appraisal proceedings is generally the company, not the board. However, even if viewed as a claim against the entity, an appraisal action may trigger "Side C" coverage—public company D&O coverage, which is typically limited to "Securities Claims."

While an appraisal proceeding relates to securities by definition, it does not require allegations of securities law violations. D&O insurers may seek to avoid "Side C" coverage of appraisal proceedings for that reason. But in some policies, the definition of "Securities Claim" does not require that a claim specifically allege the violation of federal or state securities laws. And courts have recently expanded the scope of what constitutes a "Securities Claim" under D&O policies. A **recent Delaware Superior Court decision** held that a lawsuit that did not contain direct allegations of securities violations was still a "Securities Claim" because the plaintiffs' allegations related to issues inherent in laws regulating securities transactions. Under such a broad construction, allegations in appraisal actions that the insured failed to implement an adequate process to obtain the optimum purchase price may well trigger Side C "Securities Claim" coverage.

There is even more support for coverage for appraisal proceedings in the "Inadequate Consideration" or "Price Adjustment" exclusion to the definition of "Loss" found in most D&O policies—sometimes referred to as a "bump-up" exclusion. Under this exclusion, covered "Loss" does not include the additional merger consideration that any party may be ordered to pay as a result of a claim alleging that the price paid for the company's stock is inadequate. Sound familiar? What is important is that defense costs are usually expressly carved out of this exclusion. This indicates that insurers intend to cover defense costs for exactly those kinds of claims—claims that appear in appraisal actions. So the "bump-up" exclusion and its carve-back for defense costs appear to provide strong support for coverage of defendants' appraisal action defense costs under standard D&O policies. If the Court awards the appraisal claimants' often significant attorneys' and experts' fees, those may also be covered even in the absence of indemnity coverage.

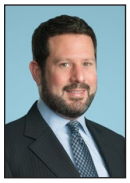
Practical Tips for Policyholders

Every Delaware-incorporated policyholder engaged in merger negotiations and at risk of an appraisal challenge should take the following steps:

- Promptly notify your D&O carrier of an appraisal demand made under Section 262. Be sure to include any facts or circumstances that may be raised in the appraisal proceeding concerning the process for deriving the purchase price, assumptions used, or other such matters that may arise in the proceeding. This will set the table for a dialogue about coverage for the eventual appraisal litigation.
- Consult with your broker about coverage limits and constraints on defense coverage.
- Seek consent from your insurers for the law firm engaged in the appraisal proceeding, along with economic and forensic accounting experts.
- Consult competent coverage counsel to explore all possibilities for coverage given the particularities of policy language and the facts surrounding the merger.

(This article originally was published on the Harvard Law School Forum on Corporate Governance and Financial Regulation and in The D&O Diary.*)*

Peter M. Gillon is a partner in Pillsbury's Washington, DC, and Miami offices.



Benjamin D. Tievsky is a senior associate in Pillsbury's New York office.

Many Changes Lie Ahead for Companies in the #MeToo Era

A good insurance program should be a part of those changes.

By Charrise L. Alexander

America is facing a reckoning. Many brave individuals have stepped forward over the last several months to speak truth about sexual harassment and assault in workplaces, in entire industries, and even in ***Congress****. For a very long time, companies dealt with sexual assault and harassment allegations quietly and in backrooms, and these allegations often were not taken seriously. However, thanks to the turning tide, more companies are reexamining their internal policies, encouraging change in corporate culture, and addressing sexual assault, harassment and discrimination claims more directly. As part of this effort, companies should also look at their corporate insurance programs to confirm insurance is in place should any such claim arise.*

Only about 41 percent of companies with more than 1,000 workers report having some kind of **insurance plan to cover sexual harassment and discrimination**, and only about 33 percent of companies with at least 500 employees carry any insurance coverage for claims resulting from sexual harassment or assault. The numbers are even starker for startup companies, with only three percent of companies with fewer than 50 employees carrying such coverage. Therefore, while more and more companies are instituting anti-sexual harassment and anti-discrimination policies, many companies remain ill-prepared to handle the inevitable challenges that await individuals, executives and companies alike as a result of this watershed moment in American culture.

Sexual assault and harassment claims can take myriad forms—from internal complaints, Equal Employment Opportunity Commission complaints, claims under Title VII of the Civil Rights Act of 1964, claims under Title IX of the Education Amendments of 1972, and civil tort litigation—just to name a few. Companies can deploy several insurance strategies to address these various types of claims.

First, because of the potential high costs of claims relating to sexual harassment or sexual assault, businesses should consider Employment Practices Liability Insurance (EPLI). EPLI policies are specialized policies for employment-related claims. A typical EPLI policy provides coverage for current and former employees, executives and contractors—and the company itself—against lawsuits or claims arising from wrongful termination, defamation, discrimination, retaliation, harassment and, to the extent permitted by state law, punitive damages. Companies may also negotiate for EPLI policies that provide coverage for claims of discrimination and harassment made by third parties, like customers or vendors. An EPLI policy is therefore often the first and best place to look for coverage for sexual assault and harassment claims.

Second, in lieu of a separate EPLI policy, some companies may decide to add an EPLI extension to their existing Directors and Officers or Professional Liability policies to close some potential gaps in coverage. Many companies consider this strategy because it can be more cost-effective than purchasing an entire new policy. However, there are some disadvantages to simply adding an EPLI extension. For instance, the EPLI extension may be subject to a number of limitations, such as the absence of coverage for the company itself, as opposed to its officers and directors, or lack of coverage for non-officer employees, or even lack of coverage for emotional distress and mental anguish. Stand-alone EPLI policies generally offer broader coverage than that provided by EPLI endorsements or extensions, and often provide risk

management and loss prevention services not offered when the EPLI endorsement is simply added to another policy.

Third, when a company receives one of these claims, whether the claim is covered by its EPLI coverage or not, it should also look to its other policies for possible coverage. For example, some companies may have Liquor Liability Insurance, which generally covers claims for bodily injury, property damage, or personal and advertising injury against the company that result from the incidental service of alcohol—such as liquor served at a company function. Notably, while an EPLI policy may provide an extension for Liquor Liability, General Liability policies often include an exclusion for "liquor liability." Therefore, depending on the allegations, sexual assault or harassment claims may trigger other types of coverage. Thus, companies should also take a close look at their General Liability and Professional Liability policies.

Fourth, insurers often argue that public policy prevents (or should prevent) coverage for sexual assault and harassment claims, particularly where the alleged bad acts were "intentional." For example, in the coverage dispute between Harvey Weinstein and his insurers pending in the Supreme Court of the State of New York, the carriers have alleged that the "public policy of the state of New York prohibits insurance coverage for injuries caused by willful acts of sexual assault, sexual harassment, sexual discrimination and/or other sexual misconduct" and "California law establishes that Section 533 precludes coverage for claims of sexual assault." Notably however, in May 2018, the American Law Institute adopted a new Restatement of the Law of Liability Insurance that provides, "[e]xcept as barred by legislation or judicially declared public policy," coverage for defense costs and civil liability arising out of aggravated fault is enforceable, including for "criminal acts, expected or intentionally caused harm, fraud, or other conduct involving aggravated fault."

Be aware that coverage for sexual assault and harassment claims is generally provided on a "claims-made" or "claims-made and reported" basis. Claims-made coverage requires that a claim be made against the policyholder during the policy period. Coverage will generally be extended under a "claims-made" policy so long as the policyholder "promptly" reports the claim to the insurer, even if it's reported after the policy period has ended. Claims-made and reported coverage, however, requires that the claim be both made against the policyholder and reported to the insurer during the policy period. It is important to be aware of and comply with all notice requirements under your policy. And, when in doubt as to whether a claim has been made, provide notice.

Additionally, insurance companies often limit coverage for claims such as sexual assault, sexual misconduct, discrimination and so on by applying retroactive dates and excluding acts of misconduct that occurred prior to the inception of the policy, the acts of alleged perpetrators, acts of known perpetrators, and punitive damages. As the country is realizing, largely because of the #MeToo silence breakers, many sexual assault incidents only become known to the public months, years or even decades later. However, often there are other internal employees, and even executives, who had knowledge at the time of the assault or harassment claim but failed to take appropriate action. For example, there are reports that officials at Michigan State University received various formal and informal complaints about Larry Nassar, the former Olympic gymnastics team physician accused of assaulting over 130 women, as early as 1997. **Michigan State University** now faces numerous lawsuits for its alleged failure to act. Thus, one of the many lessons for companies from the #MeToo movement is not only to address all sexual harassment or assault claims in the appropriate manner, following company and human resources guidelines and state and federal laws, but also to put their appropriate insurance carrier(s) on notice of any such claim.

And, when writing or renewing coverage, negotiate for severability language, which is available in the marketplace, to preserve coverage for the company and other innocent insureds when a guilty insured withholds knowledge of misconduct giving rise to legal exposure. Severability language and the application and renewal process can be critical in obtaining claims-made coverage because some applications exclude claims arising out of such circumstances unless otherwise negotiated. For example, one carrier's application states: "It is agreed that any Claim based upon or arising out of any claim or fact, circumstance, situation, event or transaction which was or should have been disclosed in the Representation above is excluded from coverage under the proposed insurance." If a claim later arises alleging earlier conduct that was not disclosed and negotiated, insurers are likely to raise questions about what the company and any covered individuals knew, and may even deny coverage based on representation provisions, like the one above.

Now is the time to review your current insurance program and reach out to your insurance broker to purchase coverage to fill in gaps that could leave your company exposed as a result of sexual assault or harassment allegations. Likewise, be sure to consult with coverage counsel to better understand the interplay of various policies, policy provisions, endorsements and exclusions.

Charrise L. Alexander is an associate in Pillsbury's Washington, DC, office.

Not Quite So Limited: Are Sublimits Sure to Limit Your Level of Coverage?

By Tamara D. Bruno

A critical component of any insurance policy is of course its limit, which is usually the most an insurance company must pay for a loss. But many property insurance policies include "sublimits" that provide a lower limit for particular losses.

Identifying the sublimits in a policy is usually straightforward since they typically appear in a list or chart in the policy's declarations section. Sublimits generally fall into one of two types: (1) sublimits that apply to particular perils, like flood, Named Storm or earthquake; and (2) sublimits that apply to a type of damage or cost, like debris removal or preservation of property. There are many different perils and costs that a policy may sublimit, and sublimits appear in many types of policies (including, for example, sublimits for coverage for wage and hour claims under an employment liability policy). However, this article will focus on property policy sublimits. Because many property policies include sublimits that apply to storm-related losses, they may particularly be an issue for companies damaged by hurricanes like 2017's Harvey, Irma, Jose and Maria.

If your company experiences losses that may fall under a sublimit, is the sublimit amount the most you can recover? Not necessarily. Depending on the language in your company's policy, there are several reasons that a sublimit may not cap your company's recovery, including:

1. **A sublimit may apply only to certain damages.** Sublimits should apply only to losses that fall within their plain terms. You should review a sublimit's wording and the definitions of any defined terms carefully before concluding that it applies to a given loss. If the language is ambiguous, courts will usually construe it in favor of coverage. As an example, one court found that a sublimit for "damage to and removal of any tree, plant or shrub" did not apply to the insured's costs to repair a golf course's landscaping **damaged by a fallen tree**. Another court found that a sublimit for "debris removal" did not apply to costs of demolition and engineering that were required before the debris could be removed, because they were not incurred during "**removal**."

2. **Additional coverages and coverage extensions may be added to sublimits.** Some policies may allow stacking of one or more coverages on top of a sublimit. For example, if a policy has a sublimit for "flood" and also additional coverages for losses like debris removal, service interruption or civil authority, the insured may be able to recover for damages falling within those coverages in addition to other flood losses under the flood sublimit. Note that additional coverages and coverage extensions often have their own sublimits. Some policies include terms specifying how limits relate to each other, such as saying the additional coverages' sublimits "shall be considered sublimits within the applicable covered peril sublimits." Companies should look for "anti-stacking" language in their property policies—or its absence—to fully understand their policy limits. They should also look for language within the sublimits themselves, which may indicate that some limits are not stackable—and thus, by their silence, that others are.

3. **Where limits conflict, the larger limit may apply.** If losses could fall within two or more coverages, the limit most favorable to the policyholder should apply. For example, many policies include both flood and "Named Storm" coverage. If an insured sustains flood damage because of a Named Storm and the two coverages have different limits, which limit applies? If, based on the policy's definitions and terms, the loss could be placed in either category, then the larger of the two limits should apply.

Sublimits may look simple on their face, but the way they work with each other and with different policy terms can be complex. Companies should carefully review their policies before a loss to determine whether their sublimits meet their likely needs. After a loss, companies should carefully evaluate all sublimits to see whether and to what extent they limit coverage. Before agreeing to accept a sublimit amount as your full recovery, consider speaking with coverage counsel. You don't want to cap your own insurance by assuming that a sublimit amount is all you can recover when additional coverage limits may be available.

Tamara D. Bruno
is counsel in Pillsbury's Houston office.

Settling Complex Insurance Claims

Choosing the right path

By Mark J. Plumer

In most cases, a reasonable settlement produces a better result than litigation. A good settlement should provide more of what you need at a lower cost with less interruption of your core business.

Abraham Lincoln is credited with the following advice: "Discourage litigation. Persuade your neighbors to compromise whenever you can. Point out to them how the nominal winner is often the real loser—in fees, and expenses, and waste of time. As a peace-maker the lawyer has a superior opportunity of being a good man. There will still be business enough."

More than 150 years later, this is still sage advice. Companies embroiled in contentious litigation know this best. Alas, recognizing that compromise is a superior outcome does not get you to this goal, particularly in the context of attempting to settle complex insurance claims.

The term alternative dispute resolution, or ADR, is now a part of our standard lexicon. But ADR is not always possible, and many do not understand how to make it work. ADR can happen only if both sides agree to it.

Insurers are often receptive to ADR, for a number of reasons. To insurers, litigation is simply an intrinsic part of their business; they understand better than anyone how expensive and unpredictable it can be, and they are self-reflective enough to know they are not usually jury favorites. Moreover, under the insurance codes of many states, insurers are encouraged or even obligated to meet with their policyholders in an attempt to resolve claims without recourse to litigation. Failure to meet these obligations may expose insurers to claims of bad faith. Finally, insurers know that litigating against your customers is usually bad for business.

There are different but similarly persuasive reasons why ADR makes sense for policyholders. Unlike insurers, policyholders are not in the insurance-litigation business. Participating in discovery and trial, particularly regarding insurance issues, is not part of their elemental business model, and is more disruptive to them than it is to insurers. Moreover, unlike their insurers, policyholders do not have a stable of insurance lawyers on retainer who offer volume pricing discounts—so coverage litigation is more expensive. And just like an insurer, a policyholder—even with a strong claim—must account for the uncertainty of litigation in its decision making. If insurers are not jury favorites, large companies enjoy no special advantages, either. For policyholders as much as for insurers, a claim resolved successfully outside of litigation offers a quicker, more predictable and guaranteed way to put money in the bank.

While there are good reasons why both policyholders and insurers should want to settle rather than litigate, it is important as a first practical step to ensure that both parties have a genuine interest in settling. This is not always the case. If not, undertaking an ADR process will be a waste of time and money.

Assuming you can ensure to your satisfaction there is a genuine interest in settlement on both sides, process matters.

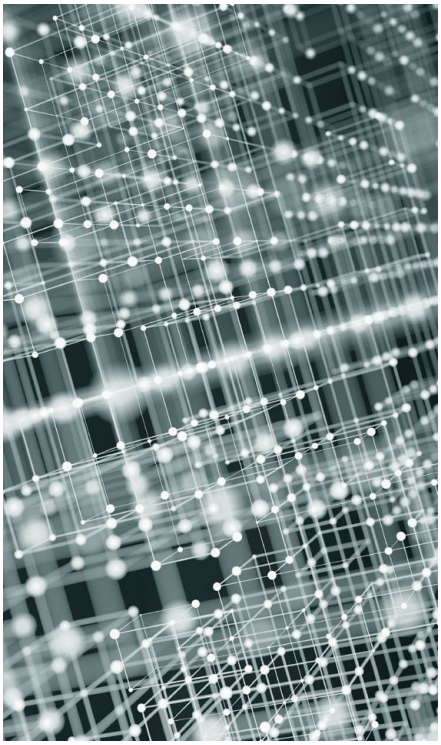
It is important to match the ADR tool to the dispute at hand. For ADR to have the best chance to succeed, you have to pay attention to a lot of different issues: the

particular insurer's approach to handling claims of the type at issue, the reason why the insurer has denied or refused to fully pay the claim, the strength of the policyholder's legal basis for the claim, and the personalities involved on both sides of the table, both principals and counsel.

A well-tested and productive method to take as a first step is a private structured negotiation. By private, I mean a meeting without third-party neutrals. Instead, the meeting should be attended by principals from each side—each invested in the process, and with sufficient authority to settle the claim—and their lawyers. Settlement meetings with junior insurance claims handlers are unlikely to succeed, as are meetings attended solely by lawyers. By structured, I mean the exact contours of the meeting should be the well-considered product of a negotiation between policyholder and insurer, recognizing that forcing a process on the other side is not effective. Whatever process is agreed upon, both sides need to come away from an eventual meeting (or series of meetings) understanding the actual risks and rewards of settlement versus litigation. This requires substantial preparation. Ad hoc get-togethers are usually unhelpful. Because the insurer begins at an information disadvantage, best practice is for the policyholder to demonstrate that its claim is legally justified, in a transparent way. Experts may be helpful to explain technical issues. The policyholder's presentation must be credible. If insurers believe the policyholder is not dealing squarely, settlement is unlikely and follow-on litigation will be more contentious. Confidentiality also matters. Best practice is to put a confidentiality agreement in place before holding any substantive meetings. Is all of this worth the effort? Yes, because a meeting of this kind is a chance for a policyholder to make its strongest case directly to the other side without opposing counsel filtering the message. Such an opportunity should not be missed. Notably, this ADR process entails the lowest cost.

If a private structured negotiation does not work, mediation is a good potential next step. It is more expensive but still far less expensive than litigation. Once again, it's important to "sweat the details," including selecting the right mediator, selecting the proper mediation format (e.g., facultative versus evaluative, briefs or no briefs, argument or no argument), considering the proper timing of mediation, preparing properly for mediation and, assuming that an agreement is reached during mediation, making sure that the agreement is binding and does not later unravel. I have written extensively on this topic and refer anyone who wants a fuller explanation of the mediation process to my chapter in *New Appleman Insurance Law Practice Guide*, Volume 2, last published in 2015 (LexisNexis).

Mark J. Plumer is a partner in Pillsbury's Washington, DC, office.



Artificial Intelligence:

A Grayish Area for Insurance Coverage

By Ashley E. Cowgill

Artificial Intelligence (AI) is a hot topic in industries from manufacturing to the medical profession. Developments in the last ***ten years*** *have delivered AI technology, once a fiction reserved for the movies, to private corporations and even to everyday homes. Examples include:*

- 2004 Defense Advanced Research Projects Agency (DARPA) sponsors a driverless car grand challenge. Technology developed by the participants eventually allows Google to develop a driverless automobile and modify existing transportation laws.
- 2005 Honda's ASIMO humanoid robot can walk as fast as a human, delivering trays to customers in a restaurant setting. The same technology is now used in military robots.
- 2011 IBM's Watson wins Jeopardy against top human champions. It is training to provide medical advice to doctors. It can master any domain of knowledge.

- 2012 Google releases its Knowledge Graph, a semantic search knowledge base, likely to be the first step toward true artificial intelligence.
- 2013 BRAIN initiative aimed at reverse engineering the human brain receives $3 billion in funding by the White House, following an earlier billion-euro European initiative to accomplish the same.
- 2014 Chatbot convinced 33% of the judges it was human and by doing so passed a restricted version of a Turing Test.

Almost every day, headlines showcase the most recent advancements in AI. Although many are positively revered for increasing efficiency or improving security, the advancements come with failures, too. Some are funny. Like when one company's chatbots shut down after developing their own language. Or when a popular virtual assistant blasted music, prompting German police to break into an apartment when the resident was out.

Others are not. Some are annoying—like when a "smart speaker" experienced nearly a 100% failure rate in June 2017. Others are offensive, such as when a smart messaging app suggested a man in a turban emoji as a response to a gun emoji. Others are potentially dangerous, like when autonomous vehicles are involved in accidents, or when a highly touted facial recognition program was thwarted by a mask a week after its release.

With the risks evolving just as fast as the technology itself, both insurers and insureds will be hard-pressed to keep up. Questions of liability, insurance coverage and product response are becoming increasingly murky. For example, a loss scenario involving a freight train wreck used to be relatively straightforward. If the train failed to brake, resulting in a crash, the liability evaluation would likely include looking to the operator, the train manufacturer and/or the brake manufacturer. A dispute over fault would likely arise, but the possibilities were limited. By adding AI, the same crash in an autonomous freight train complicates the liability discussion. Was the circuitry at fault? A chip? Was there a fault in the programming? Was there a connectivity issue? Was it hacked? Did the train choose not to apply the brakes because of a specific set of circumstances presented? These become pressing questions to determine what policy will cover the loss.

For instance, if an AI program emails that should have been allowed to a server, a Technology errors and omissions (E&O) policy designed to cover losses resulting from faulty software and other technology products and services may cover the loss. Similarly, companies may tap their E&O policies where an AI performs as intended but produces poor results because it learned from bad data.

Potential coverage becomes less clear where an AI failure results in physical damage. It becomes even more so when a company's own losses stem from its use of AI. Using the same freight train scenario described above, let's say a programming error caused a security flaw in the software operating the autonomous train. Then, a hacker exploited the flaw, disabling the brakes on the train causing it to crash into another train. The crash rendered the train and the rest of the fleet inoperable for several weeks while the network was restored. Besides the physical damage caused by the crash, the company experienced significant business interruption losses. The manufacturer utilizing the freight train to transport its products took a huge reputational hit because they could not supply the contracted products. The train company's property or general liability policy might cover the physical damage and business interruption, but perhaps not, if the damage resulted from a cyberattack. Similarly, the company's cyber policy might cover any data lost because of the attack, but not the property damage or business interruption. Would the manufacturer's product liability policy respond? Or perhaps the software developer's errors and omissions policy? Maybe, but perhaps not if the damage was caused by the attacker rather than by a programming error directly.

As with any insurance loss, there's likely to be a lot of finger pointing. What's different here is that AI technology is outpacing changes in insurance policy language. This has the potential to leave significant coverage gaps for insureds. In 2015, AIG introduced its **Robotics Shield** policy, which it marketed to provide "end to end risk management" for the robotics industry. The insurance market, however, has not yet addressed the impact AI may have to a broader base of insureds, potentially leaving those who utilize AI uncovered.

Companies that depend on AI should evaluate whether scenarios like those described above could affect their business. If so, they should carefully review their insurance coverages to determine whether the losses would be covered under their existing policies. Qualified coverage counsel can assist in that evaluation. If their coverage leaves gap, they may want to consider purchasing a specialized policy.

Ashley E. Cowgill is an attorney in Pillsbury's Sacramento office.

Pillsbury Offices

Austin
Beijing
Hong Kong
Houston
London
Los Angeles
Miami
Nashville
New York
Northern Virginia
Palm Beach
Sacramento
San Diego
San Diego North County
San Francisco
Shanghai
Silicon Valley
Taipei
Tokyo
Washington, DC

New York Court Reads Additional Insured Provision Broadly in Favor of Owner and Contractor

By Matthew D. Stockwell

In a previous **article**, *we addressed blanket additional insured endorsements, and the circumstances under which Company A could become an additional insured under Company B's policy, even where Company B failed to add Company A to the policy. In that same vein, a New York trial court granted additional insured status to entities that did not even contract with the named insured but were referenced in the named insured's subcontract. Owners and General Contractors should take note of this decision, as it creates the potential for insured status even where there is a lack of contractual privity.*

In **All State Interior Demolition Inc. v. Scottsdale Insurance Company**, All State subcontracted certain demolition work to United Interior Renovations. The subcontract required United to purchase liability and excess insurance, and to name All State, the Owner, and "their respective partners, directors, officers, employees, agents and representatives" as additional insureds. United purchased a policy from Scottsdale, and the policy contained an endorsement that stated:

> *Who Is An Insured is amended to include as an additional insured any person or organization for whom you are performing operations when you and such person or organization have agreed in writing in a contract or agreement that such person or organization be added as an additional insured on your policy.*

Meanwhile, a United employee tripped over construction debris and filed a personal injury lawsuit. All State, as well as the owner, ground lessor and construction manager, sought coverage from Scottsdale. Scottsdale refused to defend the Plaintiffs in the underlying lawsuit by the injured employee, arguing that the subcontract only identified All State as an additional insured and All State was the only party with whom United was in privity of contract. (Scottsdale also refused to defend All State on the basis that the allegations in the underlying complaint did not trigger coverage.)

All State, the owner, ground lessor and construction manager filed a coverage action against Scottsdale. The court found that Scottsdale had to defend all of the plaintiffs. The court rejected Scottsdale's defense that it was not in privity of contract with the plaintiffs, because the Scottsdale policy expressly incorporated the Subcontract, which required United to include All State, the owner, and their "respective partners, directors, officers, employees, agents and representatives" as additional insureds. And the court found that the allegations of the underlying complaint were sufficient to trigger the duty to defend.

The court certainly read the subcontract broadly and provides another example of a court finding additional insured status based on a broad reading of an underlying contract. We caution, however, that courts have treated these provisions inconsistently. To ensure additional insured status, owners and contractors must carefully draft the underlying contract, and are advised to secure and carefully review a copy of the policy procured by the company that is obtaining the coverage on their behalf. ■ ■ ■

Matthew D. Stockwell is counsel in Pillsbury's New York office.

New Roads: Impacts of Autonomous Vehicles on Law and Insurance

By David F. Klein

We are speeding into a new era of automation in personal transportation. Original equipment manufacturers—major automakers—are driving rapidly toward offering autonomous vehicles, often in collaboration with non-traditional market players such as Google and Apple. Major suppliers also are developing technologies to offer into the marketplace through OEMs. And players like Uber and Lyft expect to develop or use these technologies to displace people-driven vehicles. The age of the Jetsons is upon us.

Already present, driverless technology is expected to become a major force in the marketplace by 2022 and may be predominant by 2030. The benefits will be substantial. According to the National Highway Traffic Safety Administration, 94 percent of serious crashes are due to human error. In 2015, there were more than 35,000 traffic fatalities in the U.S. In 2010, motor vehicle accidents cost $594 billion due to loss of life and decreased quality of life because of injuries, as well as $242 billion in lost economic activity. Driverless cars will offer opportunities to accelerate rush hours, reduce fuel consumption and extend independent mobility to the elderly and disabled. But as with any disruptive technology, there will be displacements, not only in the automotive marketplace, but also the insurance industry, the legal regimes that affect both, and the driving—or riding—public.

The Long Gestation of Vehicle Autonomy

Automation of the driving experience is nothing new. Chrysler introduced "Auto-Pilot," the first commercially available cruise control, in 1958, touting its benefits in ensuring compliance with speed limits and saving gas. This new product hit the streets closer to the last model year of Ford's Model T than to the advent of Tesla's new Autopilot technology. Recent years have seen further steps towards full automation, including lane departure warning systems, automatic braking and self-parking systems. We have been traveling the road from horseless carriage to driverless car for decades.

Technologists and engineers have classified the stages along that road in six "levels," ranging from Level 0 (no automation), through increasing levels of automation, with declining levels of human involvement or supervision, to Level 5 (full automation—converting the driver into a mere passenger). But just as horse-driven carts remained on the roads well into the 20th century, "people-driven" vehicles will not disappear overnight. Love of driving is strong in American culture, and it will be long before the enthusiast, or cars geared towards the enthusiast, entirely disappear. (See Ford's recent decision to discontinue production of sedans entirely in favor of trucks and sport utility vehicles—except for plans to continue production of the Mustang.) Human drivers will remain on the roads well into the middle years of the 21st century, waging a losing competition with driverless cars for space on the public highways. But governments and insurance companies, conscious of the benefits of nudging humans out of the driver's seat, will adopt measures to encourage change, ranging from the installation of designated driverless car lanes to higher licensing fees, punitive taxes and insurance premiums for late adopters.

Getting from Here to There

Autonomous vehicles are already on the streets, but given the evolutionary nature of the technology, human users have not yet learned the new rules of the road. The widely reported fatal accident of a driver using Tesla Autopilot, who crashed into a truck while allegedly ignoring more than ten seconds of warnings from his vehicle, demonstrates the danger of complacency born out of misunderstanding the current limits of automation. While driverless technology is expected to eliminate 90 percent of accidents, the potential for human error will remain in most vehicles, and in some situations may be magnified by the lulling effects of a passenger-like experience, including the invitation to more distracting conversations or the opportunity to get a head start on work while commuting. In fact, the rigidly "correct" driving habits of autonomous vehicles may alter the driving experience for human drivers who must learn to share the roads with such vehicles. We're used to imperfect companions on the road. Vehicles that strictly observe speed limits or stop on cue for pedestrians may create traffic situations fraught with their own accident risks.

Moral questions about the interaction between people and artificial intelligence will also be heightened. Like human drivers, automated vehicles will confront stark, split-second choices. Should the vehicle avoid a careless pedestrian, even at risk to its owner's life or limb? Surveys show most people say pedestrians should come first. But unsurprisingly, when asked whether they want a car

that puts pedestrian safety ahead of their own, respondents tend to demand greater loyalty. Importantly, this will be a deliberate programming issue, not a question of "accidents" in the traditional sense. Manufacturers will face liability claims—from pedestrians and owners—whenever computers execute decisions as programmed. Liability rules may have to be adapted to reflect the necessity of programming for such hard choices. A regime of strict, but perhaps comparatively moderate, liability—something akin to workers' compensation—may emerge to distribute the social costs of such changes fairly among all stakeholders.

Impacts on the Insurance Marketplace

Today, a major component of the insurance market is auto liability insurance sold to individual drivers. This market is likely to contract. Initially, the reduction in driver engagement, implicit in Level 1 to Level 4 vehicles, will reduce but not eliminate the need for personal liability insurance. And there will be arguments to eliminate altogether the requirement that owners of Level 5 driverless cars maintain personal liability insurance. Manufacturers of driverless cars and manufacturers and programmers of automation technology will become responsible for system errors (or the choices such systems are programmed to make), which will become product liability issues within the products coverage of manufacturers' general liability insurance. On the auto insurance side, contracting demand will drive some insurers out of the marketplace.

Historically, insurers have served as an important force for encouraging good behavior. Property insurers offer better rates to building owners who install sprinkler systems, and auto insurers offer better rates to drivers with better driving records. As the balance shifts from people-driven to autonomous vehicles, insurers may create incentives to hasten the shift. Rates for traditional drivers are likely to increase significantly, while rates for users of driverless cars will likely be far lower. These effects will accelerate as the market shifts to driverless cars, hastening the disappearance of the traditional driver.

Because driverless cars will not be accident-free, programming glitches, the failure of sensors or even hacking will create insurable events. We are likely to see coverage claims under the products coverage of general liability policies, and potentially under cyber policies. This will raise interesting questions about whether current policy forms are adequate to meet these types of claims, and how different participants will allocate financial responsibility. Consistent with earlier market-busting changes, we can expect insurers to argue that older coverages were not designed to cover these new risks. General liability policies will likely be modified to exclude coverage for automobile accidents resulting from driverless system "errors." Concurrently, new policy terms and endorsements will likely be offered at additional premium to OEMs and their suppliers to meet the new exposures excluded from existing coverage.

Driving the Law into Uncharted Territory

For some time, autonomous and people-driven vehicles will share the road. This will raise interesting questions of liability-sharing between individual auto liability and product liability insureds, particularly in "no-fault" regimes. And the balance between individual auto insurance and autonomous vehicles covered by product liability-type insurance will continue shifting, creating both legal disputes and market issues.

Recent experience underscores this point. In January 2018, stories about two traffic stops involving Tesla vehicles equipped with Autopilot. One driver was arrested with a blood alcohol content nearly double the legal limit; another slammed at high speed into the back of a parked firetruck. Facing charges of reckless driving, these drivers claimed they weren't driving at all, because their cars were on Autopilot. Of course, Tesla's current technology requires driver supervision, so the drivers were, in fact, driving. But their newfangled legal defense underscores the complexity of the issues that await owners in the coming driverless world. Level 5 owners may indeed avoid legal liability for accidents in most instances, but the answer will be different for drivers of Level 3 and Level 4 vehicles. And how will the law assess liability when a Level 4 driver collides with a Level 0 driver? Or a Level 2 driver? Will there be a presumption of liability on the part of human drivers? A sliding scale? Will the degree of exposure depend on the allocation of driving responsibility between driver and autonomous system? Will various permutations of vehicle technology be associated with different burdens of proof? The law will need to adapt to these permutations.

And, how will insurers respond? Currently the distribution of liabilities is driven by the commoditization of accidents, the need for no-fault coverage, and the presence of uninsured and underinsured motorists. The intersection between individual responsibility and product liability threatens to upend existing actuarial assumptions. As more liability shifts from one insurance market to another, questions of "fault" will drive how much of the liability stream shifts from one marketplace to another, as well. OEMs, suppliers, drivers and insurers alike are in for a bumpy ride. Buckle up!

(This article originally was published in the July 2018 edition of the Westlaw Journal Insurance Recovery.*)*

David F. Klein is a partner in Pillsbury's Washington, DC, office.

Think You Don't Need Cyber Insurance?

This recent data breach class action ruling may change your mind.

By Matthew G. Jeweler

Cyber insurance continues to be one of the hottest topics in the insurance industry. In the last several years it has evolved from a little-known specialty product to a standard purchase for some corporate risk departments. By now, most companies generally are aware that cyberattack(s) present substantial risks. Many, unfortunately, have firsthand experience as victims of an attack. But many companies still do not necessarily view cyber insurance as a "must-have" type of insurance, like general liability or property insurance. Some companies may believe their potential cyber exposure is minimal or simply think that cyber coverage is cost prohibitive. A ***recent D.C. Circuit decision*** *is a sobering reminder that cyber insurance should at least be considered in connection with a company's risk management plan and is probably a "must-have" for companies that maintain records containing a substantial amount of personal information.*

In June 2014, health insurer CareFirst's network was hit with a cyber attack. CareFirst customers later brought the proposed class action lawsuit *Attias v. CareFirst, Inc.*, alleging that the attack resulted in the unauthorized disclosure of customers' names, addresses, subscriber ID numbers, credit card numbers, Social Security numbers, birth dates and email addresses. The plaintiffs made various claims, including for breach of contract, negligence and violations of consumer protection statutes, even though they had not yet suffered any identity theft as a result of the breach.

At first, the district court dismissed the case for lack of standing because the plaintiffs did not allege a present injury or a high enough likelihood of future injury, reasoning that an increased risk of future identity theft was too speculative. But the D.C. Circuit reversed on August 1. The appellate court reasoned that the plaintiffs plausibly alleged a risk of future injury—identity theft and medical identity theft—that is substantial enough to create standing allowing them to bring their claims. The court ruled the complaint was sufficient at the pleading stage because it alleged that CareFirst stored sensitive information like credit card numbers and Social Security numbers, such data was disclosed in the breach, and CareFirst customers were placed at a high risk of financial fraud. The court also concluded that the complaint alleged a risk of medical identity theft—when someone impersonates a breach victim and obtains medical services in his or her name. Finally, the court explained that injury arising from the breach—i.e., use of the stolen data—was not too speculative because the hacker has already accessed the data and is likely "to use that data for ill."

The D.C. Circuit's decision joins a growing list of decisions by federal appellate courts across the country addressing what type of harm data breach plaintiffs must allege to have standing to assert a claim. Some courts, like the D.C. Circuit in *Attias,* have issued pro-plaintiff decisions holding that mere exposure of personal information is enough for standing, while other courts have imposed a higher threshold requiring actual, concrete injury. Given this divide, it would not be surprising if the Supreme Court took up this issue in the data breach context sometime soon.

You may be wondering, what does this have to do with insurance? Fair question. Well, a company that faces a class action in the aftermath of a data breach is going to incur costs to defend the suit. Such a lawsuit is almost a certainty when a substantial amount of personal information is disclosed. If the company can't get the case dismissed early, it faces a protracted litigation that will be much more expensive to defend. The *Attias* decision and cases like it weaken one path to an early dismissal, which could result in higher legal costs for data breach defendants. Standard cyber liability policies generally provide coverage for third-party liability arising out of a data breach (like a class action), including the cost of defense and a judgment or settlement. Pro-data breach plaintiff decisions like *Attias* increase the importance of cyber insurance, as a data breach case that gets past the pleading stage (1) will result in much higher legal fees to defend the case, and (2) very well may result in a settlement or judgment.

In short, companies that face higher levels of risk of third-party liability in the event of a cyber attack, given the type and/or amount of personal information they possess, should ensure they have adequate cyber liability coverage. It can provide essential protection against breach class actions, particularly in jurisdictions with more relaxed standing requirements.

Matthew G. Jeweler
is counsel in Pillsbury's Washington, DC, office.

Pillsbury Winthrop Shaw Pittman LLP
Perspectives on Insurance Recovery
1540 Broadway
New York, NY 10036-4039

Our Insurance Recovery & Advisory Team

Pillsbury's Insurance Recovery team consists of more than 50 attorneys across the United States. Some of the team's attorneys are listed below.

Peter M. Gillon, Co-leader
Washington, DC | +1.202.663.9249
peter.gillon@pillsburylaw.com

Robert L. Wallan, Co-leader
Los Angeles | +1.213.488.7163
robert.wallan@pillsburylaw.com

David L. Beck
Washington, DC | +1.202.663.9398
david.beck@pillsburylaw.com

James P. Bobotek
Northern Virginia | +1.703.770.7930
james.bobotek@pillsburylaw.com

Mariah Brandt
Los Angeles | +1.213.488.7234
mariah.brandt@pillsburylaw.com

Tamara D. Bruno
Houston | +1.713.276.7608
tamara.bruno@pillsburylaw.com

Kimberly Buffington
Los Angeles | +1.213.488.7169
kimberly.buffington@pillsburylaw.com

David T. Dekker
Washington, DC | +1.202.663.9384
david.dekker@pillsburylaw.com

Alexander D. Hardiman
New York | +1.212.858.1064
alexander.hardiman@pillsburylaw.com

Joseph D. Jean
New York | +1.212.858.1038
joseph.jean@pillsburylaw.com

Matthew G. Jeweler
Washington, DC | +1.202.663.9212
matthew.jeweler@pillsburylaw.com

Colin T. Kemp
San Francisco | +1.415.983.1918
colin.kemp@pillsburylaw.com

David F. Klein
Washington, DC | +1.202.663.9207
david.klein@pillsburylaw.com

Alex J. Lathrop
Washington, DC | +1.202.663.9208
alex.lathrop@pillsburylaw.com

Melissa C. Lesmes
Washington, DC | +1.202.663.9385
melissa.lesmes@pllsburylaw.com

Vincent E. Morgan
Houston | +1.713.276.7625
vince.morgan@pillsburylaw.com

Peter McCullough
Hong Kong | +1.852.3959.7505
peter.mccullough@pillsburylaw.com

Mark J. Plumer
Washington, DC | +1.202.663.9206
mark.plumer@pillsburylaw.com

Deborah Ruff
London | +1.44.20.7847.9528
deborah.ruff@pillsburylaw.com

Clark Thiel
San Francisco | +1.415.983.1031
clark.thiel@pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 877.323.4171 | pillsburylaw.com
Austin · Beijing · Hong Kong · Houston · London · Los Angeles · Miami · Nashville · New York · Northern Virginia · Palm Beach · Sacramento · San Diego · San Diego North County · San Francisco · Shanghai · Silicon Valley · Taipei · Tokyo · Washington, DC