SUMMER 2017

Perspectives on Insurance Recovery

pillsbury

Welcome to the latest edition of Pillsbury's *Perspectives on Insurance Recovery*. In the past year, our practice continued to be at the forefront of policyholder-side insurance issues. And we are happy to report that our efforts have been recognized by various publications, including our selection by Law 360 as Insurance Practice of the Year -- for the second year in a row. In addition, nine of our practitioners were named as leaders in the industry by *Chambers USA, Legal 500* and *Who's Who Legal*.

In this issue, we discuss a sampling of the issues confronting our clients in a rapidly changing risk environment. This issue focuses on cybersecurity and data breaches, international issues that affect multinational companies, and continued areas of dispute involving D&O policies.

Additional examples of our thought leadership can be found on our blog, PolicyholderPulse.com, and our Twitter page, @PHPulseLaw.

Peter Gillon and Robert Wallan
Co-leaders, Insurance Recovery & Advisory

ARTICLE HIGHLIGHTS

Do Recent Events Make You "Wanna Cry"?

Massive ransomware attacks are just another reason to have robust cyber insurance in place.

By James P. Bobotek, Peri N. Mahaley

On May 12, a massive ransomware cyber-attack infected over 100,000 computers in more than 150 countries. This malware, a Trojan virus known as "WannaCry," "WanaCryptor," or "Wcry," encrypts files, and then threatens to destroy them, unless the victim pays a ransom. As of May 14, WannaCry had victimized at least 200,000 users in more than 100,000 organizations, including the UK's National Health Service, global shipper FedEx, Chinese universities, Russia's Interior Ministry, Telefonica, Gas Natural and Iberdrola, and Renault. The attack, which continues to spread, reinforces the need to procure cyber insurance, and to ensure that coverage extends to exposures resulting from ransomware attacks.

What is WannaCry?

WannaCry takes advantage of a vulnerability in older versions of Windows, including Windows 7 and Windows XP. In March, after the NSA discovered the "EternalBlue" exploit that would later be used by WannaCry, Microsoft issued a security update that prevents WannaCry

and other malware from affecting computers and networks using Windows 7. However, many Microsoft users did not upload the patch. Further aiding the hackers is the fact that, while Microsoft no longer supports Windows XP, many still use it. Or, as is common in some Asian countries, users are running pirated versions of Windows and are afraid to run updates and risk discovery. As a result, computers without security patches for the various Windows versions in use are common in some areas, and easy prey for WannaCry.

Those in control of WannaCry seek ransom payments in the form of Bitcoin. The initial ransom demand starts at $300, with a threatened increase to $600 if not paid within 3 days. The hackers claim that, absent payment within 7 days, the encrypted files will be deleted and all data not backed up elsewhere will be forever lost.

WannaCry is indiscriminate in its end product. It is unfocused on a distinct target or trade. Even worse, it is designed to spread throughout systems that have not taken appropriate defensive measures. Remarkably, it can spread through networks without users taking any action.

What Is Ransomware?

Ransomware is a form of malicious software that penetrates computer systems or networks and uses tools like encryption to deny access or hold data hostage until the target pays a ransom, frequently in Bitcoin. A ransomware attack is typically delivered via an e-mail attachment which could be an executable file, an archive or an image. Once the attachment is opened, the malware is released into the user's system. It can be in the form of encryption (individual PCs or a server), lock screen, or mobile device (typically affecting Androids).

The infection is not immediately apparent to the user. The malware operates silently in the background until the encryption mechanism is deployed. Then, a dialogue box appears that tells the user the data has been locked and demands a ransom to unlock it again. By then it is too late to save the data through security measures.

Ransomware attacks are on the rise—there are now more than 50 families of this malware in circulation—and it is quickly evolving. With each new variant come better encryption and new features. This is not something to ignore. One of the reasons why it is so difficult to find a single solution is because encryption in itself is not malicious. In fact, many benign programs use it.

Do Not Despair—There Is an Insurance Product that Covers Many Ransomware Damages.

The necessity of cyber insurance in some form or another cannot be questioned today. Most cyber insurance policies offer various grants of coverage on an à la carte basis. One of these grants is commonly referred to as "cyberextortion" or "ransomware" coverage. Typically, this coverage will pay for: (i) the money necessary to meet the ransom demand; (ii) the costs of a consultant or expert to negotiate with the extortionist; and (iii) the costs of an expert to stop the intrusion and block future extortion attempts. Another commonly available coverage, typically referred to as "business interruption" or "time element" coverage, may cover lost business income arising from an attack.

What Should You Do if You Are the Victim of a Ransomware Attack?

Notify your insurers immediately. Some cyber insurance policies provide coverage only for costs incurred after the insured notifies the insurance company. Some policies also require that the policyholder inform the applicable law enforcement agency and obtain the insurer's consent before making any ransom payment. Therefore, despite the urge to move swiftly in response to this crisis, we recommend policyholders understand and comply with the notice provisions of their policies in order to preserve their right to insurance coverage.

Consider whether you will pay the demanded ransom. Paying the ransom is tempting, but there is no guarantee that paying will actually lead to your files being decrypted. In addition, you are supporting the criminal's business model and thus are partly responsible for more and more people getting infected with ransomware.

Document your losses. Properly documenting your losses is crucial. Establish separate accounts to track losses, including any extra expenses, professional fees, mitigation costs, and other expenses associated with the attack. Keep a log of all actions taken. Save all receipts and other records of additional expenses.

Engage. It is usually prudent to engage professional claim consultants, such as forensic accountants, particularly where there is business interruption loss. Additional experts may be needed to model the unique financial aspects of your business. Their professional fees and other mitigation expenses are frequently covered under cyber/privacy policies, subject to sub-limits, and usually subject to carrier pre-approval. It is also a good idea to retain an experienced insurance coverage lawyer, not just when you need an advocate, but to help you protect the privileged nature of your communications and to avoid many of the traps for the unwary when presenting your insurance claim. Counsel may work in the background, without revealing their involvement to carriers. Carriers usually do the same thing. Cooperate with the insurance company adjuster, but don't forget they work for your insurer, not for you. If you need an advocate, hire your own.

What Can You Do to Prevent a Ransomware Attack?

Confirm that all of your computers and networks are current with security updates. Windows users should confirm they have the latest Windows security updates installed, and should only use

(continued on page 10)

The Cyber Crystal Ball

Is There Insurance Coverage for the Top Threats of 2017?

By Peri Mahaley

Cyber sages tell us the question is not whether your business will suffer a data breach, but when. To prepare for the inevitable, businesses want to know what is the next threat on the horizon. In the past few months, experts have offered many views on the top cyber trends for 2017, and plenty of advice about security measures companies should take in light of these predictions. But if some loss is a given, businesses also want to know if there will be insurance to cover that loss. We look at some of the forecasts and try to answer that question.

In its Fourth Annual Data Breach **Industry Forecast**, Experian Data Breach Resolution, a vendor of data breach response and protection services with a track record of handling high-profile incidents, issued and identified five top data breach trends for 2017.

Aftershock Password Breaches

Experian predicts that companies will increasingly experience the impacts of previous data breaches as username and password information obtained in earlier attacks are sold and resold on the dark web. Companies affected could include not only those who were the victims of the original attack, but unrelated businesses in cases where consumers have used the same usernames and passwords for multiple accounts. Massive breaches like the hack of one billion Yahoo user accounts heighten this risk exponentially.

Specialized cyber risk insurance policies are the principal source of coverage for these kinds of events. Both the cost of defense and damages arising from third-party claims alleging the unauthorized access to or disclosure of personally identifiable information (PII), including protected health information (PHI), fall within the core coverage of these policies. The costs of responding to a breach—notification costs, call center costs, crisis management expenses and credit monitoring—also typically are covered. Coverage for fines and penalties payable to the payment card brands such as Visa and Mastercard is available but usually for an additional premium. Coverage for lost income due to a network or business interruption caused by the breach may also be purchased.

But the aftershock scenario presents special problems. With respect to the victim of the original attack, the insurer is likely to take the position that any claims or losses attributable to a breach that happened years ago relate back to the original incident and are not covered under a current policy. Although the company may look to the policy that was in place when claims were first asserted, the limits of that policy may already have been exhausted or released by prior settlement. A company that did not experience a breach directly but suffers loss or claims because of fraudulent use of credentials previously stolen from a different company faces an even greater challenge. Its coverage may be triggered only by a security failure affecting its own network, or the unauthorized access of information within its own custody or control. And finally, there is no coverage for long-term effects on the business of breach victims, like the negative impact on the Yahoo-Verizon deal.

Nation-State Attacks – Transition from Espionage to War

Experian forecasts an escalation of cyber conflicts between countries, evolving from espionage to open conflict and perhaps even war. In Experian's view, collateral damage for consumers and businesses is inevitable, while industries responsible for critical infrastructure are particularly vulnerable.

Two areas of concern emerge on the coverage front. The first is the fact that most cyber policies contain some form of exclusion for loss arising out of acts of war by foreign states, military action, insurrection, revolution, and the like. But thus far, where foreign state actors were known or suspected to be responsible for cyber-attacks, the incidents have not risen to the level of war or military action. In addition, many such exclusions have cyber-terrorism exceptions, which have served to preserve coverage for the scenarios to date. If Experian's prediction is correct, however, insurers likely will deny coverage more frequently on the basis of the war exclusion.

The second concern is that coverage for loss due to cyber-attacks on critical infrastructure may not be covered under standard cyber policies. Most policies provide coverage for loss arising out of the failure of the security of the policyholder's computer system to prevent unauthorized access or use, but "computer system" often is not clearly defined to include operational or industrial controls. Many infrastructure attacks to date have targeted precisely these types of systems (e.g., the 2015 attack on two Ukraine power distribution companies and the takeover of the control system of a German steel mill in 2014), and can be expected to do so in the future. Coverage is available in the marketplace for these types of events and should be explored, especially by companies whose continued operations are essential to public safety.

We started answering the question whether specialty cyber policies are likely to respond to two of the top five cyber threats for 2017 identified by Experian Data Breach Resolution in its **industry forecast.** In this one, we examine the remaining three.

Continuing Health Care Sector Attacks

Experian predicts that the health care sector will continue to be the most targeted sector, with more attacks on hospital networks, and more thefts of electronic health records. Ransomware will continue to be a top concern, with a shift in emphasis from blocking access to systems to stealing information to sell or leverage for identity theft. In addition, recent Office of Civil Rights guidance has noted that ransomware attacks may be classified as breaches requiring notification under HIPAA, adding significantly to the cost implications of such events.

Coverage for cyber extortion is often provided in cyber policies, but the extent of coverage varies widely. While some policies limit coverage to the actual ransom payment, others cover a broad range of related expenses, such as the costs of investigating the validity and severity of the threat, hiring independent negotiators, and protecting against further threats. Until recently, notification of affected individuals may not have been required for extortion events and therefore was not included in coverage. Health care systems in particular should ensure that they purchase the broadest extortion coverage possible in light of these new requirements.

Focus on Payment-Based Attacks

Experian believes that hackers will continue to focus on obtaining payment card information in 2017. Although EMV chip technology (named for its original developers Europay, MasterCard, and Visa) is available to prevent against point-of-sale (POS) fraud, adoption of the new technology has been uneven. U.S. retailers lag behind their overseas counterparts—this despite the fact that the major payment networks are shifting more liability for fraudulent transactions from the card issuers to merchants who do not use chip-enabled devices. Meanwhile, attackers continue to find new techniques to steal payment card data en masse using POS skimmers.

As noted previously, coverage is available for fines, penalties, and other assessments that must be paid to the payment card brands under card servicing agreements, but it is not automatically offered in a standard cyber policy. Policyholders who process credit card payments should obtain this specialized coverage. In addition, they should pay close attention to the specifics of the coverage. Some policy wording limits coverage to claims asserted by the card brands themselves, when in fact the direct obligation may be to the intermediate payment processor, who in turn is required to indemnify the card brand. Policyholders must also make sure that a standard policy exclusion for loss arising out of contractual assumption of liability or general breach of contract does not eviscerate the payment card liability coverage. Ideally, the coverage will include legal costs incurred in responding to payment card claims and the costs of any forensic investigation required by the card brands.

Big Headaches for Multinational Companies

The most damaging attacks are expected to be those involving the loss of international consumers' data, in large part because the proliferation of new rules regarding response plans and notification standards. The EU's General Data Protection Regulation (GDPR) and new regulations poised to take effect in Canada and Australia will complicate matters and increase costs for multinationals. International consumers who are not used to being notified of breaches may be more vocal, and may stop doing business with companies in the wake of a breach.

The costs of notifying consumers as required by law or regulation—domestic or foreign—are generally covered by cyber policies, but companies may want to revisit the adequacy of their policy limits. And while companies can purchase coverage for income lost during a suspension or interruption of operations due to a breach, coverage is not generally available for

business that is permanently lost as a result of consumer lack of confidence.

While coverage for all of these eventualities may not be available today, more will be available tomorrow as the risks become better understood and better managed. More importantly, companies should be proactive in pushing their brokers and insurers to provide insurance products that meet the known threats head-on.

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

New Cybersecurity Regulations from the NY DFS: What Every Insured Should Know

By Tamara D. Bruno

The vaults of the world's financial capital are getting stronger locks. On March 1, 2017, new "first-in-the-nation" **cybersecurity regulations of the New York Department of Financial Services (DFS)** *went into effect to protect consumers and the financial system from cyber attacks. While the regulations apply to covered finance and insurance companies, their influence is likely to be felt beyond the companies targeted initially. For this reason, it's important that all companies with cybersecurity risks understand how the new DFS regulations work, and the insurance coverage issues they may raise.*

The Regulations

New York's new cybersecurity regulations apply to banks, insurers and other financial services institutions licensed in New York, with limited exceptions for smaller companies, captive insurance companies and others. The regulations' requirements generally fall into a few categories:

- **Cybersecurity Programs:** Covered entities must establish and maintain cybersecurity programs designed to (i) identify cyber risks, (ii) establish and test defenses to protect non-public information from cyber risks, and (iii) detect, respond to and recover from cybersecurity events. The technical requirements are detailed and include both annual penetration testing and bi-annual vulnerability testing.

- **Third-Party Vendors:** Covered entities are responsible for their third-party vendors' protection of non-public information. Covered entities must identify risks from third-party access, impose minimum cybersecurity practices for vendors, and perform due diligence in evaluating the vendors.

- **Management Responsibility:** The regulations make clear that responsibility for cybersecurity starts at the top, saying in the introduction: "Senior management must take this issue seriously and be responsible for the organization's cybersecurity program." Covered entities are required to designate a Chief Information Security Officer (CISO), who must report to the board annually. The board or a senior officer must annually attest that the company is in compliance with the regulations.

- **Reporting Requirements:** Covered entities must disclose within 72 hours to the Secretary of the DFS any cyber security event that either (i) must be disclosed to another government or self-regulating agency, or (ii) has a "reasonable likelihood of materially harming any material part" of the company's normal operations. Cybersecurity events subject to disclosure include unsuccessful cyber invasion attempts.

Coverage Issues

While the regulations don't directly relate to cyber or liability insurance, there are several ways they could have an impact on such insurance:

- The regulations could open covered entities up to potential liability from regulatory actions or consumer litigation in the event of a compliance failure or cybersecurity event. Such companies should make sure that their cyber and/or other liability policies provide coverage for such claims.
- The responsibilities imposed on management could also lead to claims against directors and officers of covered entities, for example for alleged misrepresentations about the strength of the company's cyber protections. Covered entities should make sure that their D&O policies don't exclude such cyber risks—either specifically, implicitly, or as part of broad cyber exclusion.
- The regulations' third-party vendor requirements could also expose covered entities' vendors to potential liability and may create issues as to whose policy should respond to a given claim.

Even for non-covered entities, the New York regulations may serve as a standard for protecting third-party information. Their requirements or similar requirements may come to be applied more broadly, whether by contract or regulation. Companies that are not subject to the regulations should still take care to understand their requirements and insurance impacts for when they need to secure their own safes.

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

Think Globally:

Insurance Analysis for Multinational Companies

By Joseph D. Jean and Janine M. Stanisz

Insurance is not only a risk transfer tool, but also a valuable asset. Certain coverages, however, are not purchased or pursued by multinational companies transacting business in the United States because there are nuanced differences between international and U.S. insurance programs and law. These companies, often with global offices, will be best served by having counsel experienced in such nuances conduct a diagnostic review of their insurance policies. Not only may potential coverage gaps be identified, but a company will be better able to plan ahead and negotiate more favorable coverage terms before a loss arises.

1. What risks does your business face, and are you insured for such losses?
At the most basic level, a company must consider not only the risks it potentially faces, but also the assets that it must protect, and then optimize the structure of its insurance program accordingly. Different types of policies cover different types of risk (e.g., general liability, property damage, directors and officers

liability). It is imperative to understand how your insurance program will operate in the event of a loss. Consider whether any assets remain unprotected.

Think broadly—not all assets are tangible. For example, companies have recognized the exposure they face when it comes to network and data security breaches. The cyber insurance market has skyrocketed, but cyber policies are far from uniform. There is room for negotiation. Know what you need and what you don't, so that you're able to negotiate effectively for what you want.

(See our earlier **10 Tips for Negotiating Your Cyber Insurance Policy** posts.)

2. Will your policies' limits of liability protect your business? Consider whether your insurance policies' limits of liability adequately cover your specific business, and plan for the worst. Pay attention to sublimits. For example, a first-party property policy may have much smaller limits for certain events, such as floods or storms. If a loss were to occur, would your business have adequate property, liability, and business interruption coverage and limits?

Depending on the size of the organization, companies may have many different layers of insurance, e.g., primary, umbrella and excess policies. The umbrella and excess policies supplement the dollar amount of coverage afforded by primary policies by providing coverage above the limits of the primary coverage. Once your primary policy is exhausted, these umbrella or excess layers of insurance should provide additional coverage. Umbrella and excess policies sometimes allow insurers to offer coverage at lower premiums by permitting insurers to diversify their risks, thereby limiting their exposure.

Operating in the United States can be challenging because the liability landscape can be vastly different than in other countries. Knowing your business, the liability risks it faces, the states in which it operates, as well as the various regulatory schemes governing its operations and markets can help you identify the correct types and limits of insurance you need. Speak with your broker and qualified counsel to help you identify these risks and how to both mitigate and transfer them.

3. Have you complied with state-specific insurance mandates? Some businesses are statutorily required to purchase certain types of insurance. For example workers' compensation and automobile liability insurance usually are mandatory, and these types of policies are intended to benefit third parties, rather than the company directly. Unlike most other forms of insurance, a company's insurance needs may vary state-by-state. A company that fails to abide by the applicable statutory framework may face steep fines and penalties. Not only must a company consider what risks it seeks to protect, but it must also understand the state-specific differences in insurance law.

When considering your insurance program and negotiating a policy renewal, understanding how relevant insurance policies have been interpreted is essential. Understanding your company's policies' terms can save time and money in the event of a loss. Work closely with your insurance broker and a coverage lawyer to ensure that your risk transfer mechanisms will work efficiently and effectively when you need them.

Joseph D. Jean is a partner in Pillsbury's New York office.

Janine M. Stanisz is an associate in Pillsbury's New York office.

Pillsbury's Insurance Team Named a *Law360* Practice Group of the Year for the Second Year in a Row

With a focus on consequential matters and overall excellence, the award recognizes practices that have accomplished the biggest wins between October 2015 and October 2016.

Among the many notable insurance-related outcomes identified by *Law360* was Pillsbury's successful $72 million jury verdict for client Lion Oil Co. The decision – deemed the largest insurance jury verdict in 2015 by *National Law Journal* – was led by 2016 *Law360* Insurance MVP Geoffrey Greeves and Pillsbury Insurance practice co-leader Peter Gillon. The same team is currently advising Sinclair Oil in an approximately $100 million dispute against Swiss insurer Infrassure for property damage and business interruptions incurred due to an explosion in Cheyenne, Wyoming. After the defeat of the insurer's initial motion to dismiss bad faith claims, the case is expected to go to trial later in 2017. In California, Insurance practice co-leader Robert Wallan is heading a team litigating coverage and bad faith for more than $100 million in products liability class and mass actions against Fluidmaster. Trial in that case is set for December 2017, and the court already has ruled in the client's favor on summary judgment that Fireman's Fund owes a duty to defend. As of July 2017, we've recovered $30 million in defense fees, contributions to underlying settlements, and *Brandt* fees from some of the insurers.

"It's an honor to be selected as Insurance group of the year two times in a row," said Gillon. "This track record of recognition reflects how committed we are to our clients, to representing policyholders against insurance companies and to continually achieving great results for them."

According to practice co-leader Robert Wallan, Pillsbury is regularly involved in high-profile cases because it is "one of the few major law firms in the nation dedicated to representing policyholders and not liability insurers."

Pillsbury exclusively represents policyholders against their insurance companies and has become one of the largest and most respected Insurance Recovery & Advisory practices in the United States. The group has been lauded by *Chambers USA, The Legal 500 U.S.* and *Best Lawyers*.

Who Cares about an Oxford Comma? A Maine Dairy Receives a $10 Million Lesson in Grammar and Ambiguity

By Peter M. Gillon and Janine M. Stanisz

A panda is sitting in a bar, polishing off his dinner. He pulls out a gun, fires a shot in the air, and heads toward the exit. A stunned waiter demands an explanation. The panda pauses at the door and tosses the waiter a badly punctuated wildlife manual. "I'm a panda—look it up." The waiter turns to the appropriate entry: "Panda. Large black-and-white bear-like mammal, native to China. Eats, shoots and leaves." [1]

Beware the missing Oxford comma!

That was the lesson of a recent decision by the First Circuit Court of Appeals, which held that the omission of an Oxford comma in a Maine employment statute created an ambiguity that must be resolved in favor of dairy delivery drivers. For want of a comma, the dairy is out $10 million.

The Maine overtime statute states that an employer cannot force an employee to work more than 40 hours a week unless the employee is compensated 1½ times his or her regular hourly rate for work performed in excess of 40 hours. Certain categories of workers, however, are excluded, including employees who fall within Exemption F:

> The canning, processing, preserving, freezing, drying, marketing, storing, packing for shipment or distribution of:
>
> (1) Agricultural produce;
> (2) Meat and fish products; and
> (3) Perishable foods.

26 M.R.S.A. § 664(3)(F). At issue was whether dairy drivers, who do not typically pack perishable foods, but instead simply transport them, fall within the above overtime exemption. The dairy drivers successfully argued they do not.

The holding hinged on the meaning of "packing for shipment or distribution"—more specifically, how to interpret this clause when there was no comma preceding the words "or distribution." With the comma, they likely would have lost. Without it—taking into account interpretative aids, the law's purpose and legislative history, statutory construction, and non-binding case law from the Maine Superior Court—the court reasoned, Exemption F was at best ambiguous. The dairy drivers were therefore entitled to overtime.

To an insurance coverage attorney, this opinion is not revolutionary, but is rather further confirmation of general insurance policy interpretation principles. Clear and unambiguous terms in an insurance policy are given their plain and ordinary meaning. If, however, an ambiguity exists, such that the language is susceptible of more than one reasonable interpretation, the court must look to the intention of the parties and the policy should be interpreted in favor of the policyholder. Exclusions must be narrowly construed, and the insurer bears the burden to show that the exclusion is clear and unmistakable, subject to no other reasonable interpretation, and applicable to the facts presented in the case at issue. The First Circuit applied these same principles when analyzing Maine's overtime statute.

In a recent insurance case our firm handled, **Lion Oil Company v. National Union Fire Insurance Company of Pittsburgh, PA**, the structure and use of clarifying punctuation in the policy resulted in the insurer's liability for "service interruption coverage" when an oil refinery's crude oil supply line burst, leading to large contingent business interruption losses for the refinery. In that case, a federal district court acknowledged that the service interruption coverage part was ambiguous as written and found in favor of coverage.

Whether you're a coverage nerd like us, or just a grammar enthusiast, do not underestimate the power of an Oxford comma. Without it, invitations like "I'm starving, let's eat Grandma" could be extremely hazardous.

[1] Based on an old joke and the basis for Lynn Truss' book, *Eats, Shoots & Leaves: The Zero Tolerance Approach to Punctuation.*

Peter M. Gillon is a partner in Pillsbury's Washington, DC office.

Janine M. Stanisz is an associate in Pillsbury's New York office.

Pillsbury Office Locations

Abu Dhabi
Austin
Beijing
Dubai
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
Tokyo
Washington, DC

A Subcontractor's Defective Work Is an Occurrence: *Weedo* Wobbles... and Falls Down

By Stephen S. Asay

Since 1979, commercial general liability (CGL) insurers have relied on the New Jersey Supreme Court case of Weedo v. Stone-E-Brick Inc. *and its progeny to argue that a subcontractor's defective work can never qualify as an "occurrence" under a standard form ISO CGL policy. This argument is contrary to both the language of standard CGL policies and the trend in recent case law, but courts in New Jersey and elsewhere have continued to cite* Weedo *for this proposition. With its new decision in* **Cypress Point Condominium Association Inc. v. Adria Towers LLC,** *the New Jersey Supreme Court has now finally relegated* Weedo *to its proper status as an historical footnote based on outdated policy language.*

Cypress Point involved claims for rain water damage to a condo building. When the condo association began noticing the damage, it brought claims against the developer/general contractor and several subcontractors. The association alleged that the subcontractors' defective work on the exterior of the building allowed water leaks that damaged steel supports, sheathing and sheetrock, and insulation. When the developer's CGL insurers refused to cover the claims, the association sued the insurers, seeking a declaration that the association's claims against the developer were covered.

Relying on *Weedo*, the insurers argued that they were not liable because the defective work was not an "occurrence" that caused "property damage" as defined by the policies. The New Jersey Supreme Court was thus tasked with

determining whether rain water damage caused by a subcontractor's defective work constitutes "property damage" and an "occurrence" under a standard form ISO CGL policy. Properly applying the policy language, the court held that a subcontractor's defective work that causes damage is an "occurrence" under the plain language of the policy.

Discussing the evolution of the standard form ISO CGL policy, the court recognized important distinctions between the 1973 and 1986 versions. (Variants of the 1986 version are still in widespread use today.) First, the 1973 definition of "occurrence" incorporated a requirement of resulting property damage; that requirement was removed from the 1986 definition. Second, and more importantly, the 1973 policy did not include the "subcontractor exception" to the "your work" exclusion. This exception, which was included in the 1986 policy, represented an agreement between policyholders and insurers "that the CGL policy should provide coverage for defective construction claims so long as the allegedly defective work had been performed by a subcontractor rather than the policyholder itself." Because *Weedo* involved the 1973 CGL policy, the New Jersey Supreme Court rejected the insurers' contention that *Weedo* has any bearing on coverage under the 1986 CGL policy.

Turning to the language of the 1986 insuring agreement, the court first determined that the damage caused by the rain water leaks clearly met the definition of covered "property damage." The court then addressed the definition of an "occurrence"—i.e., "accident"—under the policy. Applying common definitions, the court found that an "accident" includes "unintended and unexpected harm caused by negligent conduct." Because the result of the subcontractors' defective work—water damage to non-defective portions of the building—was an "accident," it was a covered "occurrence" under the policy.

After determining that the insuring agreement provided coverage, the court turned to policy exclusions raised by the carriers. (This is an important analytical step skipped by many courts, which sometimes overlook the incredibly broad coverage provided by the insuring agreement.) While the "your work" exclusion applied, the damage claimed by the association arose out of subcontractors' defective work. Therefore, the "subcontractor exception" to the "your work" exclusion restored coverage for the association's claims.

The New Jersey Supreme Court's decision that damage caused by a subcontractor's defective work constitutes an occurrence (and covered property damage) is consistent with both the plain language of the 1986 standard form ISO CGL policy and the strong trend in case law around the country. Thanks to the *Cypress Point* decision, insurers can no longer rely on *Weedo* to argue against coverage for such damages. Perhaps even more importantly, *Cypress Point* leaves open the question of whether the standard CGL policy covers defective work itself where there has been "property damage" beyond the mere existence of a defect. Both the policy language and the original intent of the subcontractor exception support such coverage, and the court's reliance upon those considerations may indicate that New Jersey courts will find further coverage available for construction defects under the standard form CGL policy.

Stephen S. Asay is an associate in Pillsbury's Washington, DC office.

Do Recent Events Make You "Wanna Cry"? *(cont. from page 2)*

fully-supported software. Failure to do so could impact coverage under many policies.

Implement application "whitelisting." Only allow systems to execute programs known and permitted by your security policy.

Secure backup. Make certain that you have secure data backup to media not connected or mapped to a live network.

Implement incident response plans. Address distributed ransomware attacks and perform "tabletop" exercises tailored to ransomware scenarios.

Don't Let It End in Tears. Aside from enterprise risk management endeavors such as vigilance, secure data backup to media not connected or mapped to a live network, disabling macros, and diligent installation of software updates and patches, inclusion of cyberextortion coverage as part of your cyber insurance program is not only recommended, but is gaining acceptance as a best practice in today's commercial risk management world. Not having it in today's world will surely make you WannaCry.

James P. Bobotek is a partner in Pillsbury's Washington, DC office.

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

New York High Court Gives the Bronx Cheer to Insurers' Pro Rata Allocation and Exhaustion Arguments

By Benjamin D. Tievsky

Over time, New York's courts have erected multiple barriers to policyholders seeking to recover insurance for long-tail, progressive injury claims—such as environmental or asbestos liabilities—that can implicate multiple policies over multiple policy terms. Now, in a New York minute, just weeks after hearing oral argument, the Empire State's highest court has leveled the playing field by endorsing the "all sums" and "vertical exhaustion" approach to allocation advocated by a policyholder, at least as to policies containing "non-cumulation" and "prior insurance" provisions.

In *In re Viking Pump, Inc.*, New York's Court of Appeals did not overrule its 2002 decision in *Consolidated Edison Co. of New York v. Allstate Ins. Co.*, which had applied pro rata allocation where the non-cumulation clause argument was not raised, but the court made clear that pro rata allocation is not the default rule in New York. Rather, the specific wording of the triggered policies will control, and can require allocation on an all-sums basis. This is a huge win for policyholders with New York liabilities and a further endorsement, by a prestigious court, of the "all sums" approach to allocation.

This was a battle royale. Insurers threw in the kitchen sink in their attempt to preserve the New York Court of Appeals' previously-rendered pro rata ruling in *Consolidated Edison*. They retained Kathleen Sullivan, a preeminent appellate lawyer and former Dean of Stanford Law School, to argue their cause. Many amicus briefs were filed.

The Court of Appeals handed down its *Viking Pump* decision on May 3. The case involved insurance for asbestos-related personal injury liability. The Delaware Supreme Court, which was reviewing a lower Delaware court decision under New York law, certified two questions to the New York court: "(1) whether 'all sums' or 'pro rata' allocation applies where the excess insurance policies at issue either follow form to a non-cumulation provision or contain a non-cumulation and prior insurance provision, and (2) whether ... horizontal or vertical exhaustion

is required before certain upper level excess policies attach." The New York court unanimously answered in favor of "all sums" and "vertical exhaustion"—just as the policyholder requested.

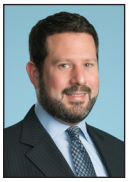
With respect to allocation, the insurers argued that their liability to cover the underlying damage should be allocated pro rata over multiple policy years—in proportion to each insurer's respective "time on the risk." The policyholder urged that each insurer was jointly and severally liable for the entire loss, citing each policy's promise to cover "all sums" the policyholder was obligated to pay as damages, as well as the policies' non-cumulation or prior insurance provisions, which sought to collapse coverage for other policy years into each insurer's policy. The Court of Appeals properly held that these types of provisions explicitly contemplated that the policies would cover damages occurring before and after the policy period, not merely "during the policy period," as the insurers argued. Indeed, the court found such provisions "incompatible" with pro rata allocation. Without repudiating *Consolidated Edison*, the court relied on specific policy wording and declined the insurers' invitation to make pro rata allocation the default rule in New York.

With respect to exhaustion, the insurers argued that excess coverage could not be triggered in *any* policy year until all "underlying" primary and umbrella coverage had been exhausted in all policy years. The policyholder argued that excess coverage in a given policy year is triggered as soon as the underlying primary coverage in that year is exhausted. Once again, the court agreed with the policyholder, holding that the attachment language of the excess policies supported vertical exhaustion, which it also found conceptually consistent with all sums allocation.

The practical effect of *Viking Pump* is profound. Where the language permits, it allows policyholders to maximize recovery for long-tail claims by:

- Avoiding allocation of the loss across uninsured periods, gaps in coverage, policies sold by now-insolvent insurers, and policies containing problematic exclusions; and
- Accessing high-level excess coverage without having to exhaust many successive years' worth of primary policies (and often, multiple significant self-insured retentions).
- An example illustrates the benefits. Imagine a policyholder with a long-tail environmental claim where New York law applies. The site operated for 50 years, but only 10 years of insurance are available, and in 5 of those years, the policies contain pollution exclusions barring coverage. Under a pro rata approach, the policyholder can recover no more than one-tenth of its damages (5 years of available coverage for a 50-year loss). But in an all sums allocation, the policyholder can target any one of the 5 years of available coverage and place the entire loss—vertically—into that single year. Depending on available limits, the policyholder may recover 100 percent of the loss.

Historically, non-cumulation clauses and prior insurance provisions were common in umbrella and excess policies, as well as policies sold by certain industry mutual insurers. Policyholders vulnerable to long-tail claims should scrutinize their policies, as well as the allocation and exhaustion law in their jurisdictions. Other insurance provisions and excess policy attachment language should be given a fresh look in light of this recent decision.



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

The D&O Cramdown:

Triggering Side A DIC Coverage When an Underlying D&O Carrier Declines Coverage

By Peter Gillon and Eric M. Gold

A great deal of premium exchanges hands to buy the Difference in Condition (DIC) or "drop-down" component of excess Side A DIC coverage. Yet policyholders, brokers, and to a large extent, D&O liability carriers, have surprisingly little understanding of just how that standard coverage feature is triggered—or how it works in practice. Recent experience with the drop-down provision suggests that it can be a highly valuable tool to help resolve disputes in which one or more carriers is refusing to meet its coverage obligations. But triggering the coverage is fraught with difficulties.

A Side A DIC policy typically sits excess of a traditional Side ABC D&O policy, providing an additional layer of protection and limits for individual directors and officers, which cannot be consumed by claims against the insured entity via Side B (indemnifiable claims) and Side C (direct claims against the entity). It is intended to fill in several important gaps for individual D's & O's:

1. It provides excess Side A D&O insurance when a company's traditional Side ABC tower is exhausted or is voided due to rescission.

2. It provides excess coverage to D's and O's when their company is unwilling, or financially unable, to advance or indemnify the cost of defending a claim, or satisfying a judgment or settlement of a claim, such as in the case of a bankruptcy liquidation.

3. It drops down to provide defense and indemnity when underlying policies exclude coverage, based on, e.g., an "insured versus insured" exclusion or a "pollution exclusion," and the insured entity fails or is unable to provide indemnity.

4. It drops down to pay a claim that is not indemnifiable by the corporate entity, such as in a derivative suit, where an underlying insurer rightly or wrongly fails or refuses to pay, attempts to rescind coverage, or becomes insolvent.

It is with respect to the fourth category—where the Side A DIC policy is designed to immediately fill in for underlying carriers who refuse or fail to pay in a derivative action—that this coverage is particularly interesting.

No indemnification for derivative actions.

Corporate by-laws, reflecting State corporate laws, normally prohibit indemnification of a corporate director or officer with respect to derivative claims, i.e., claims brought derivatively in the name of the corporation against such individuals.

The prohibition on indemnifying corporate D's and O's against derivative claims avoids the circularity of a company having to indemnify the defendants against the company's own claims. Because D's and O's cannot be indemnified by their company for derivative claims, insurance for such claims is extremely important. And any potential gaps must be insured. Thus the need for Side A DIC coverage.

Triggering Language under Side A DIC Policies

One of the pioneers of the excess Side A DIC market is CODA, a division of Ace (now Chubb), and its policy wording serves as a useful reference. The Insuring Agreement in the CODA Premier policy form insures "any portion of . . . Loss" that insureds are legally obligated to pay due to Claims first made during the policy period that "is not paid under the Underlying Insurance" because the "insurer(s) of the Underlying Insurance:

(i) refuses in writing to indemnify the INSUREDS; or

(ii) fails to indemnify the INSUREDS within sixty (60) days after a written request by or on behalf of the INSUREDS for such indemnification."

(iii) See Policy, at 1.

This is the "drop-down" or DIC feature of the policy, and it makes clear that coverage can be triggered automatically and immediately by (i) a failure of an underlying D&O insurer, including any member of a Side ABC tower, to agree to a written demand for indemnity within 60 days, or (ii) by any outright declination in writing of a request for indemnity. This immediate and automatic drop-down provision is designed to protect the individual D's and O's when they need it most, such as when a settlement has been reached in the underlying litigation and carrier funding, or assurance of funding, is critical to the settlement.

The 60 day window for the underlying carrier to step-up and indemnify the insureds can be particularly helpful if, for example, a Side ABC carrier takes the position that a proposed settlement is "unreasonable," and declines to provide consent. In that case, the policyholder may issue a written request to the recalcitrant carrier for indemnity, and if indemnity is not provided within 60 days, the Side A DIC carrier may be asked to fill in the gap.

Of course, if the Side A DIC carrier meets its drop-down obligations and drops down to provide coverage, it then has a right of subrogation against the recalcitrant underlying carrier. I like to call this the "cramdown" provision, because once the DIC coverage is called upon, the Side A DIC carrier has a huge incentive to use all tools at its disposal to force the underlying carrier to reverse its declination and pay. In practice, as a result of this "cramdown" pressure, the Side A DIC carrier persuade the underlying carrier to pay, in order to obviate any payment obligation. This may not be the case where the underlying carrier has a valid defense to coverage. It is not difficult to imagine the heated negotiations that ensue when the Side A DIC carrier is asked to fill in for a solvent, underlying Side ABC carrier—regardless of the reason.

Practical Considerations

A number of issues may arise when a policyholder is considering declaring a DIC event and calling on its Side A DIC coverage.

First, when is the claim actually ripe? Frequently, coverage disputes will arise long before an underlying action is adjudicated or settlement negotiations are completed. An underlying Side ABC carrier may reserve rights to object to a final settlement on a number of grounds without actually "refusing to indemnify," leading to uncertainty as to whether that coverage will be available, yet falling short of the concrete written denial arguably needed to trigger the Side A DIC coverage. Similarly, if a Side ABC carrier declines coverage, but will not put that declination in writing as a refusal to indemnify, 60 days is a by time to wait before coverage is triggered—especially in the heat of settlement negotiations.

Second, when a DIC claim is ripe and presented to the Side A DIC carrier, the carrier may assert the same defenses as the underlying carrier. For example, some Side A DIC policies include a "reasonable consent" to settlement

clause that could be argued to preclude coverage for a settlement reached prior to declaring a DIC event. Such a position would contradict the very purpose of the DIC trigger (immediate, automatic protection for individual D's and O's when the underlying carrier fails to indemnify); and certainly the right of the DIC carrier to pursue subrogation against the non-performing underlying insurer should protect the DIC carrier from any prejudice in this regard. The same would be true of an "uninsurable loss" defense or the defense of a failure to protect the insurer's rights to subrogation, or any of the limited number of exclusions in the policy. In reality, there is no valid reason the Side A DIC policy should have any exclusions beyond a personal conduct/final adjudication exclusion and a narrow insured vs. insured exclusion (such as the version found in the CODA policy.).

Considering these practical issues, policyholders and brokers would be well-served to clarify the language of drop-down clauses. They should likewise negotiate to remove consent to settlement provisions, onerous duties in connection with subrogation rights, all but one or two exclusions, and "insurability" exceptions to the Loss definition. Also, to avoid disputes over 60-day window or consent clauses, it helps to keep Side A DIC carriers "in the loop" on discussions with Side ABC carriers and on settlement efforts in the underlying litigation. These steps may help minimize the strain of a D&O cramdown.

Peter M. Gillon is a partner in Pillsbury's Washington, DC office.

Eric M. Gold is a senior associate in Pillsbury's Washington, DC office.

If You Promise the Moon, You Must Deliver

Court Rules Insurers Must Advance Verizon's Defense Costs Under D&O Policy's Broad Definition of "Securities Claim"

By Bryan J. Coffey and Geoffrey J. Greeves

In **Verizon Communications v. Illinois National Insurance Company,** *a group of D&O insurers essentially asked, "When is a securities claim not a 'Securities Claim'" (as defined in their policies)? And a Delaware Superior Court judge effectively answered, "Never." Judge William Carpenter Jr. rejected the insurers' crabbed reading of the term "securities claim" under their D&O policies, awarding Verizon some $48 million in defense costs the insurers had withheld.*

The case arose from Verizon's decision in 2006 to spin off its print directory subsidiary, Idearc. After Idearc filed for bankruptcy protection US Bank, as Idearc's bankruptcy litigation trustee, sued Verizon and a Verizon executive who was Idearc's sole director at the time of the spin-off, asserting claims of promoter liability and breach of fiduciary duty, payment of an unlawful dividend under Delaware corporation law, and fraudulent transfer under U.S. bankruptcy law and Texas statute.

Before the spin-off, Verizon and Idearc purchased primary and excess run-off liability policies that included individual (Side A) and entity (Side B & C) coverage from the defendant insurers. The policies allowed for unallocated Side B and Side C coverage for any loss, including defense costs "incurred while a Securities Claim... is jointly made and filed against both [an] Organization and one of more Insured Person(s)." The policies defined "Securities Claim" to include "a Claim made against any Insured Person: (1) alleging a violation of any federal, state, local or foreign regulation, rule or statute regulating securities...." Verizon tendered the US Bank suit to the insurers, who agreed to advance only its executive's defense costs (but never actually paid them during the underlying lawsuit). The carriers refused to make fee advances to Verizon because, they asserted, the suit did not qualify as a Securities Claim. Verizon and its executive jointly defended the suit and ultimately

succeeded in defeating all counts against them.

After discovery in the action seeking D&O coverage, Verizon moved for summary judgment on the advancement of defense costs. The central issue as framed by the court was whether the suit by US Bank alleged "a violation of any... regulation, rule or statute regulating securities." Verizon argued for a broad interpretation, claiming (1) that "rule" should be understood to include common law rules that dictate the conduct of fiduciaries; and (2) that any law that "must be followed to properly engage in a securities transaction" is securities-related. The insurers argued that a Securities Claim could only arise out of a violation of specific federal securities statutes or state equivalents.

The court sided with Verizon. It rejected the insurers' argument that the doctrine of contra proferentem (interpreting ambiguous policy terms in favor of coverage), was unavailable to Verizon as a large, sophisticated company with its own insurance department. It held the presumption available unless it is shown that the insured had a hand in drafting the language at issue. The court also found that dictionary definitions supported Verizon's interpretation of undefined policy terms, reasoning that the insurers could have excluded common law rules and laws from the definition of "Securities Claim" had they wanted.

But it was underwriting-related discovery that provided the most ample ammunition for the court to decide against the insurers. Forms used by the primary insurer years earlier included a definition of "Securities Claim" that in fact did limit those claims to rules and regulations promulgated under the 1933 and 1934 Securities Acts, and similar state and foreign laws. Later, that definition was broadened to include violations of any law, "whether common or statutory." Then the definition was changed a second time to the broad language at issue in the case—omitting any express restriction on what laws apply—and was accompanied by marketing materials that billed the policy as an "expansion" over prior language that provided "enhanced coverage for securities liability." The court also relied on a letter produced in discovery where the primary insurer's adjuster acknowledged that another suit against Verizon alleging breaches of loyalty and fiduciary duty appeared to meet the definition of Securities Claim.

Policyholders can be expected to use this decision to potentially broaden entity coverage for lawsuits under the "securities claim" rubric. Policyholders should review this court's reasoning, and, if necessary, take steps to discover insurance companies' salesmanship in marketing attractive policy wordings. Work with your broker and an insurance law professional to carefully review your policy language for undefined terms and broad language in definitions and coverage grants to maximize the coverage you purchased. Remember, if they promise to cover a "Securities Claim," they'd better deliver.

Bryan J. Coffey is an attorney in Pillsbury's Washington, DC office.

Geoffrey J. Greeves is a partner in Pillsbury's Washington, DC office.

Our Insurance Recovery & Advisory Team

Pillsbury's Insurance Recovery team consists of more than 30 attorneys across the United States. Some of the team's partners 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
Washington, DC | +1.202.663.8930
james.bobotek@pillsburylaw.com

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

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

Geoffrey J. Greeves
Washington, DC | +1.202.663.9228
geoffrey.greeves@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

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@pillsburylaw.com

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

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

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

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

Perspectives on Insurance Recovery – Summer 2017

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 877.323.4171 | pillsburylaw.com

Abu Dhabi · Austin · Beijing · Dubai · 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 · Tokyo · Washington, DC