

The



# PRACTICAL GUIDANCE

Journal

## RANSOMWARE ISSUES IN THE HEALTHCARE INDUSTRY

Cybersecurity and Data Privacy  
in Commercial Real Estate

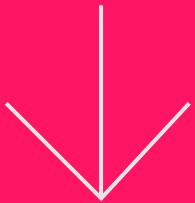
Oil & Gas Market Trends



LexisNexis®

Summer 2022

Lexis+™



# EXPERIENCE RESULTS.

**A new era  
in legal  
research.**

You don't just need the right answer—you need it right now.

**Lexis+ delivers exactly what you need with speed and clarity, so you can spend more time putting insights and analysis into practice.**

→ [LexisNexis.com/LexisPlus](https://www.lexisnexis.com/LexisPlus)

## Practice Trends

### 04 RANSOMWARE ISSUES IN THE HEALTHCARE INDUSTRY

*Healthcare*

### 15 CYBERSECURITY AND DATA PRIVACY IN COMMERCIAL REAL ESTATE

*Real Estate*

## Drafting Tips

### 29 RULES, RULES, RULES . . . CONTRACT LAW IS AWASH IN RULES (THAT TOO MANY ATTORNEYS DON'T KNOW)

*Commercial Transactions*

## Practice Notes

### 37 WHISTLEBLOWER COMPLAINT RESPONSE AND DEFENSE STRATEGIES

*Labor & Employment*

### 53 WAGE AND HOUR ISSUES RELATED TO REMOTE AND HYBRID WORK: A FERTILE DELTA FOR LITIGATION

*Labor & Employment*

### 57 EXPUNGEMENT AND REEXAMINATION PROCEEDINGS UNDER THE TRADEMARK MODERNIZATION ACT

*Intellectual Property & Technology*

### 64 CIVIL LITIGATION PROCESS MAP

*Civil Litigation*

### 70 TIMING IS EVERYTHING: THE IMPACT OF TRANSACTIONS ON PENDING BIDS AND PROPOSALS

## Market Trends

### 76 OIL AND GAS TRANSACTIONS: MARKET TRENDS

*Capital Markets & Corporate Governance*

## Advancing The Rule of Law

### 88 UKRAINE INVASION RESOURCES

To review previous editions of the **Practical Guidance Journal**, follow [this link](#) to the archive.

# 04



# 15



# 76



MANAGING EDITOR **Lori Sieron**  
DESIGNER **Jennifer Shadbolt**

CONTRIBUTING EDITORS

Bankruptcy **Mark Haut**  
Capital Markets **Victor Cohen**  
Corporate Counsel **Carrie Wright**  
Employee Benefits & Executive Compensation **Bradley Benedict**  
Finance **Robyn Schneider**  
Financial Services Regulation **Celeste Mitchell-Byars**  
Insurance **Karen Yotis**  
Healthcare **Rodney Miller**  
Intellectual Property & Technology **Miri Beiler**  
Labor & Employment **Elias Kahn**  
Life Sciences **Jason Brocks**  
Energy, Oil & Gas **Cameron Kinvig**  
Real Estate **Kimberly Seib**  
Tax **Rex Iacurci**  
ASSOCIATE EDITORS **Maureen McGuire**  
**Mia Smith**  
**Shannon Weiner**  
**Ted Zwayer**



**EDITORIAL ADVISORY BOARD**

Distinguished Editorial Advisory Board Members for The Practical Guidance Journal are seasoned practitioners with extensive background in the legal practice areas included in Practical Guidance. Many are attorney authors who regularly provide their expertise to Practical Guidance online and have agreed to offer insight and guidance for The Practical Guidance Journal. Their collective knowledge comes together to keep you informed of current legal developments and ahead of the game when facing emerging issues impacting your practice.

**Andrew Bettwy, Partner**  
Proskauer Rose LLP  
Finance, Corporate

**Julie M. Capell, Partner**  
Davis Wright Tremaine LLP  
Labor & Employment

**Candice Choh, Partner**  
Gibson Dunn & Crutcher LLP  
Corporate Transactions,  
Mergers & Acquisitions

**S. H. Spencer Compton, VP,  
Special Counsel**  
First American Title Insurance Co.  
Real Estate

**Linda L. Curtis, Partner**  
Gibson, Dunn & Crutcher LLP  
Global Finance

**Tyler B. Dempsey,  
General Counsel**  
REPAY

**James G. Gatto, Partner**  
Sheppard, Mullin, Richter &  
Hampton LLP  
Intellectual Property, Technology

**Ira Herman, Partner**  
Blank Rome LLP  
Insolvency and Commercial Litigation

**Ethan Horwitz, Partner**  
Carlton Fields Jordan Burt  
Intellectual Property

**Glen Lim, Partner**  
Katten Muchin Rosenman LLP  
Commercial Finance

**Joseph M. Marger, Partner**  
Reed Smith LLP  
Real Estate

**Matthew Merkle, Partner**  
Kirkland & Ellis International LLP  
Capital Markets

**Timothy Murray, Partner**  
Murray, Hogue & Lannis  
Business Transactions

**Michael R. Overly, Partner**  
Foley & Lardner  
Intellectual Property, Technology

**Leah S. Robinson, Partner**  
Mayer Brown LLP  
State and Local Tax

**Meredith French Reedy, Partner**  
Moore & Van Allen PLLC  
Financial Services

**Scott L. Semer, Partner**  
Torys LLP  
Tax, Mergers and Acquisitions

**Lawrence Weinstein,  
Sr. Counsel, Technology  
Transactions**  
ADP

**Kristin C. Wigness, Sr. Counsel**  
McGuireWoods LLP, Finance,  
Restructuring & Insolvency

**Patrick J. Yingling, Partner**  
King & Spalding  
Global Finance



**FROM DAY ONE OF THE RUSSIAN** invasion of Ukraine, support for the Ukrainian people in their struggle against Russia has been overwhelming. Recently, Mike Walsh, CEO of LexisNexis Legal & Professional (LNLP), announced several initiatives undertaken by LNLP and the LexisNexis Rule of Law Foundation to lend support. Resources are available to help you stay current on legal issues related to sanctions, shortages, and humanitarian impacts resulting from the invasion of Ukraine. Learn about assistance efforts, such as support for aid organizations to scale up life-saving programs and continued development of company products, solutions and projects that are focused on helping citizens and strengthening legal infrastructures in the Ukraine and elsewhere.

Oil and gas markets are experiencing volatility due to impacts from sanctions

on Russia, skyrocketing inflation, and other political and economic factors. Until recently, low outside investment and lower demand caused by the pandemic led to decreased activity in the oil and gas industry. Deal activity increased in 2021 and growth potential remains likely in 2022. Review market trends in oil and gas transactions from 2021 through the first quarter of 2022, including deal trends with respect to capital markets and M&A transactions. Read about legal and regulatory changes and get an outlook on oil and gas transactions for the future.

Also heating up is the amount of cyber-criminal activity impacting everything from the largest corporations, businesses, and industries to individual victims. Because of the types of information it possesses, the healthcare industry is a particularly valuable and vulnerable target for cyber thieves.

Learn more about the issues associated with ransomware attacks on healthcare institutions, how healthcare institutions can mitigate or prevent such an attack, and how ransomware attacks intersect with the HIPAA Breach Notification Rule.

Another business segment facing many of the same cybersecurity threats as other sectors is commercial real estate. Gain insight on some of the key issues to consider when evaluating cybersecurity and data privacy practices for your commercial real estate landlord-clients. Plus, learn critical steps to take to mitigate the risk of unauthorized release or exposure of data in their possession.

Stay current on emerging trends in Labor & Employment, Commercial Transactions, Intellectual Property & Technology and other practice areas in this edition of the Practical Guidance Journal.

## Our mission

*The Practical Guidance Journal is designed to help attorneys start on point. This supplement to our online practical guidance resource, Practical Guidance, brings you a sophisticated collection of practice insights, trends, and forward-thinking articles. Grounded in the real-world experience of our 850+ seasoned attorney authors, The Practical Guidance Journal offers fresh, contemporary perspectives and compelling insights on matters impacting your practice.*



Nathan A. Kottkamp WILLIAMS MULLEN

# Ransomware Issues in the Healthcare Industry

This article discusses market trends in 2021 relating to disclosures of climate change risks and mitigation by public companies, which are intertwined with environmental, social, and governance (ESG) issues.

**RANSOMWARE IS THE CURRENT HOT TOPIC IN CYBER-**security because its reach is essentially universal. Driving this trend, in economic terms, is that the value of having access to data often exceeds the price that could be assigned to the data itself, regardless of the industry. Because of the types of information it possesses, the healthcare industry is a particularly valuable and vulnerable target. This article discusses issues associated with ransomware attacks on healthcare institutions. It provides in-house and outside healthcare counsel, as well as compliance professionals, with a concise understanding of the mechanics of a ransomware attack and steps healthcare institutions can take to mitigate or prevent one. Furthermore, it explains how ransomware attacks intersect with the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule and how HIPAA's Security Rule can inform a healthcare institution's ransomware response plan.

## Overview of Ransomware Attack Methodologies

Given the ubiquity of digital operations, any entity with data—pretty much every organization in the modern economy—is a potential ransomware target. Complicating things further, cybersecurity teams are frequently playing catch-up to the tools that cybercriminals are developing. Moreover, technology is one piece of the puzzle, but it is not the largest piece. The biggest factor is people. Indeed, human error, inattention, and gullibility drive most cyber incidents. In fact, at least one security analyst has concluded on two separate occasions<sup>1</sup> that human error may be a contributing factor in 49%–95% of all data incidents. And, while human error may be reduced with various initiatives, it is sure to be a persistent threat.<sup>2</sup>

Because of this collection of factors, successful information management requires constant vigilance by entities in overseeing their personal and cultural operations. In other words, cybersecurity is not simply a technical matter.

## Leveraging Fraudulently Obtained Information

Following a successful system compromise, cybercriminals have three key options for next steps:

- Stealing and selling data
- Establishing financial fraud schemes
- Holding the entity hostage

Since the first two options often require considerable follow-up work and leave more detailed cyber footprints, the overall effort involved makes them less attractive for many cybercriminals. By contrast, with comparatively little effort, a cybercriminal can hold a target hostage by encrypting its data, preventing the target from accessing or using it.

Of course, the above options are not mutually exclusive. Although data may be locked as an initial matter to extract a ransom payment, the very same data subsequently may be sold or used for some sort of long-game fraud arrangement. As a result, entities may experience ransomware attacks, pay ransoms, obtain access to their data again, and resume normal operations, only to learn that the cybercriminals are still in their systems, are selling the stolen information, or are using the original information to perpetuate some sort of secondary fraud.

## Use of Digital Currency

The evolution of digital currencies has accelerated underlying fraud. Among other things, the use of cryptocurrency substantially increases the ease of receiving ransom funds compared to traditional methods of exchanging or laundering large amounts of money. Cryptocurrency also makes it easier to sell stolen information on the dark web. Notably, the dark web consists of unindexed websites that are accessed via specialized browsers that inherently frustrate the ability to track transactions.

## Size of the Attack

Matters of scale also impact how ransomware attacks are conducted. Because cybercriminals use the same basic technical tools and methods to compromise security systems regardless of target, they have an inherent incentive for aiming high and going big. Indeed, headlines abound with news about ransomware attacks that are massive and audacious. The widely publicized Colonial Pipeline ransomware attack, caused by a compromised password<sup>3</sup> found on the dark web, crippled the supply of gasoline along the East Coast for six days in May 2021.

Conversely, small entities may be easier targets for straightforward get-in-and-get-out attacks. The frequency of such smaller attacks is difficult to measure. Companies likely do not report them for myriad reasons, including embarrassment and a sense that small incidents will not merit law enforcement attention. Thus, cybercriminals are incentivized to launch multiple small attacks in the hopes of staying undetected.

1. IBM Global Technology Services, *IBM Security Services 2014 Cyber Security Intelligence Index* (May 2014); IBM Security, *IBM Study Shows Data Breach Costs on the Rise: Financial Impact Felt for Years* (July 23, 2019). 2. IBM Security, *Cost of a Data Breach Report 2020* (July 2020). 3. The Daily Beast, *Colonial Pipeline Hack Result of Single Compromised Password* (June 4, 2021).

## Heightened Risks for Healthcare Institutions

While any business can rightfully say that having swift access to its data is essential to its survival, in the healthcare context, swift access to data is often also essential to patient survival. In other words, aside from creating operational and economic challenges, ransomware attacks on healthcare entities put lives at direct risk of serious harm, including death. For example, without immediate access to health information, healthcare providers may face one or more of the following scenarios:

- They may not be aware of a patient's life-threatening allergy.
- They may have to delay time-sensitive cancer treatment.
- They may be unable to operate various essential pieces of equipment, including life support systems.

Significantly, an active case<sup>4</sup> currently working through the courts expressly asserts causation between a ransomware attack and a baby's death. According to the lawsuit, a multiday ransomware attack on Springhill Medical Center (Alabama) in 2021 compromised a wide array of the hospital's systems, including its fetal monitors. The attack allegedly led to the hospital's failure to detect complications with one of its pregnant patients, resulting in the baby's death nine months after birth. Regardless of where this particular case lands, subsequent lawsuits undoubtedly will continue to test whether healthcare entities should have liability if their operations are compromised, and patient care is impacted as a result.

### Value of Information

If the above issues relating to patient care are not troubling enough, there is a compounding issue with healthcare information: the value of health information in the criminal marketplace exceeds that of financial information. Whereas account numbers, passwords, and other financial information can be changed, health history and genetics are evergreen. Therefore, a ransomware attack on a healthcare institution could result in an operational disruption. But it could also lead to long-lasting fraud if the cybercriminals capitalize on healthcare data and operational systems as well as the underlying data within them.

For example, with patient-specific information, it may be possible to set up a fraud scheme involving phantom community-based services, which are difficult to track even when the services are real. Furthermore, cybercriminals may take advantage of intimate knowledge of an entity's invoicing system to engage in long-term fraud in which real patient information is used to submit fictional claims. Depending on how aggressive the cybercriminals are, they may be able to operate undetected for a long time.

### Sources of Data

Finally, hospitals and other large healthcare entities are often massive, with multiple service lines, diverse operational units, and fragmented data systems. This combination of factors can make it particularly challenging to maintain cohesive data governance practices. With weak data governance practices, it may be difficult to identify any particular system compromise and implement swift incident response. Without solid data governance, entities are effectively inviting false reimbursement submissions, fake supply chain invoicing, and payroll fraud, among other things.

For these reasons, cybercriminals have significant leverage to extract ransoms when they compromise healthcare information.

## Mitigation and Prevention Strategies

Just as every person is at risk of an acute health issue that could arise with little warning, all entities should operate as if they are the next target.

### Take Immediate Action

As a preliminary step, you should implement the following initiatives immediately and update them regularly:

- **Preventive.** Repeatedly educate employees about the fundamental ways in which digital systems can become compromised, particularly how the majority of compromises involve basic gullibility and human error.
- **Operational.** Maintain a robust system of backups, redundancies, and data segmentation to substantially reduce the impact of an attack.
- **Practical.** Contract for robust cyber insurance coverage to help mitigate the costs of managing an attack.
- **Strategic.** Have a plan regarding payment:
  - **The maybe pay plan.** If the entity anticipates a willingness to pay, it should consider, in advance, the following variables: the amount of the ransom, how it will assemble the funds, whether anyone in the organization has cryptocurrency experience, whether it will use a broker, whether it will attempt to negotiate the ransom amount, and its payout limit.
  - **The probably not pay plan.** If the entity plans not to pay, it should consider the following actions: its strategies for and alternatives to operating without the original data, what kind of messaging it will provide to patients and business partners while its systems are compromised, and its public image management if the ransomware attack becomes prominent in traditional or social media.



Of course, the entity should be ready to be dynamic and change the plan. To that end, it is wise to recall Mike Tyson's apocryphal quip: "Everybody has a plan until they get punched in the mouth." Without a doubt, a ransomware attack is certainly like a punch to the mouth and being nimble will be essential to avoiding a complete knockout.

Given the perpetual evolution of technology, routine maintenance and use of these strategies can make the difference between an attack resulting in a minor injury and a fatal blow.

### Employ Third-Party Resources

Even the best internal cybersecurity team can benefit from seeking outside help after an incident. On the technical front, you should consider using third-party forensics teams. These teams can assist in the following ways:

- Restoring systems
- Identifying any latent risks
- Implementing preventive measures

On the strategic front, however, expert and law enforcement recommendations and experiences vary. As a result, you might not obtain straightforward or consistent advice. Remarkably, even the FBI does not take a strong position; instead, per the National Cyber

Investigative Joint Task Force,<sup>5</sup> it offers passive guidance: "The FBI does not encourage paying a ransom to criminal actors."

Reaching out to law enforcement is always a good idea, but you should be realistic in your expectations. In the *Colonial Pipeline* case, the Department of Justice<sup>6</sup> was able to recover a significant portion of the ransom, but it is hard to imagine that government-assisted ransom recoveries will be the norm. Smaller entities, in particular, may find that there are limited law enforcement resources to assist with any recoupment efforts. Thus, while reporting matters to law enforcement may help address future threats across the industry, it may not actually help current victims. In this way, reporting may be akin to organ donation, where nothing can be done to bring back the patient, but some good can still come from the death.

To be sure, seeking strategic assistance is recommended, but you should realize that you may be faced with a range of options, each with its own limitations and drawbacks. Furthermore, some consultants may be unable to offer anything more than generic advice that requires considerable amounts of internal resources to make the advice actionable. Accordingly, you should perform your due diligence, and consult with internal experts, before retaining any outside assistance. Doing this will ensure that any chosen measures fit within your entity's budget, culture, and operating structure.

4. The Wall Street Journal Online, *A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death* (Sept. 30, 2021).

5. Ransomware: What It Is and What to Do about It. 6. U.S. Dept. of Justice, *Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 7, 2021).

## Consider Whether Payment Will Resolve the Issue

Dealing with ransomware would likely be much simpler if the ransom payment always resulted in prompt system restoration with no lingering effects. Of course, the reality is far more complicated. Among other things, the paradoxical notion of being able to trust cybercriminals to honor their words further complicates the strategies for incident response.

In any situation, there is a significant risk that the cybercriminals will take a victim's money but not return or release the ransomed data. A related risk is that paying a ransom in the first place may increase the likelihood of being a repeat victim. For example, cybercriminals may believe that payment once signals a willingness to pay again.

Furthermore, if too many cybercriminals fail to return or restore data, or launch too many subsequent attacks, victims may be more likely to behave as if their data is lost forever or that the infiltration will be a chronic issue. These scenarios reduce the overall utility of paying ransoms.

Put another way, ransomware can be like the situation of a virus that kills its host. Of course, with so many actors and the vast array of response options, even if only a fraction of all victims decide to pay a ransom, ransomware is likely to remain a threat for a long time.

## HIPAA Breach Notification Rule Requirements

Healthcare entities must also understand their obligations to notify affected individuals following ransomware attacks. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has taken the position, in its ransomware Fact Sheet,<sup>7</sup> that all ransomware incidents involving protected health information (PHI) must be evaluated under the HIPAA Breach Notification Rule. Under the Breach Notification Rule,<sup>8</sup> an entity must notify affected individuals of any breach of their PHI unless the entity can show a low probability that the PHI has been compromised.<sup>9</sup> Breaches are defined as any impermissible acquisition, access, use, or disclosure of PHI that compromises its security or privacy.<sup>10</sup> Notice to individuals typically must be made within 60 days of discovery of a breach.<sup>11</sup> Significantly, although it is possible to analyze an incident under the Breach Notification Rule and conclude that it is not a breach, as discussed in the following section, it is inherently difficult to overcome the presumption of a breach that is expressly built into the rule.

## Conducting Breach Analyses under HIPAA

To determine whether a low probability of compromise exists, a healthcare entity that sustains a ransomware attack must perform a risk assessment that considers, at a minimum, the following four factors:

- The nature and amount of PHI involved, including the types of identifiers and the likelihood the individuals can be identified from the data
- The cybercriminals who obtained the PHI
- Whether the cybercriminals actually acquired or viewed the PHI
- The extent to which the risk to the PHI has been mitigated<sup>12</sup>

Unless, using the criteria above, the entity can definitively conclude in good faith that there is a low probability that PHI was compromised, then a breach is presumed to have occurred and notice must be provided to affected individuals. Because the risk assessment requires the entity to make a judgment call, the

...entities may be faced with the difficult choice of providing expensive and potentially image-damaging notice about an event that may not actually have compromised patient information. Alternatively, they risk a significant enforcement penalty if OCR learns about the incident and disagrees with their breach risk assessment conclusions.

conclusions an entity might reach from the inquiry can be complex, highly varied, and differ from one entity to the next.

Consider, for example, a relatively straightforward ransomware incident in which cybercriminals use a basic encryption code to lock up a healthcare entity's data system. Consider further that there is no evidence the cybercriminals exfiltrated the data, the data was swiftly restored after the ransom was paid, and there is no evidence of lingering malware. Was this a breach under HIPAA requiring notification to individuals whose PHI was involved? Unfortunately, there likely is not a singular answer.

Thus, entities may be faced with the difficult choice of providing expensive and potentially image-damaging notice about an event that may not actually have compromised patient information. Alternatively, they risk a significant enforcement penalty if OCR learns about the incident and disagrees with their breach risk assessment conclusions.

## Large-Scale Breach Considerations

Healthcare entities must also notify OCR of all breaches of PHI.<sup>13</sup> For breaches involving fewer than 500 people, OCR requires only that the entities report the breaches within 60 days of the end of the calendar year in which the breaches occurred.<sup>14</sup> However, for breaches affecting 500 or more people, entities must provide notice to OCR at the same time they notify the affected individuals.<sup>15</sup> OCR posts to its website all breaches affecting 500 or more people.<sup>16</sup>

Furthermore, although OCR retains discretion to investigate any breach of any size, OCR has stated that it will "investigate all reported breaches involving the PHI of 500 or more individuals."<sup>17</sup>

Finally, when a breach involves more than 500 people in a single state or jurisdiction, the entity must further notify media outlets serving that state or jurisdiction.<sup>18</sup> To put all of this in perspective, it means that in the event of a large-scale breach, a healthcare entity is required not only to deal with what is likely one of its worst events ever, it is required to immediately disclose it to both OCR and the media so that the event can be investigated and publicized.

In addition, separate from HIPAA, entities must consider whether any particular incident implicates state breach notification laws as well.

## Subjective Standards in Determining Breaches

As noted above, the breach risk assessment factors are subjective, and the analysis is performed by the entity itself. As a result, the possibility arises that similar incidents may result in different strategies upon analyses by different entities. In the health context, consider for example a condition that has a low risk of harm, but such rare harm is catastrophic. Consider further that the treatment for this condition results in nearly universal serious side effects. In this hypothetical, some people might choose to live with the condition rather than undergo the treatment, whereas others might choose the treatment despite its side effects. Each person would make the decision based on an independent analysis of the severity and likelihood of the risks each choice presents. Likewise in the case of ransomware attacks, some healthcare entities may determine that the low risk of a major OCR enforcement action—based on their breach risk assessments—is more acceptable than the high risk of a costly public image nightmare.

## HIPAA Security Rule Risk Analysis Criteria

Whereas the HIPAA Breach Notification Rule may be difficult to apply consistently, the HIPAA Security Rule provides clear requirements for healthcare entities that can be used to plan for and prevent ransomware attacks. The Security Rule<sup>19</sup> requires healthcare entities to adopt "appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security" of electronic PHI (ePHI). Notably, it mandates that healthcare entities conduct periodic risk analyses to assess "the potential risks and vulnerabilities" to the PHI they hold.<sup>20</sup>

As a testament to its universality, HHS issued the Security Rule in 2003 and has not substantively or structurally revised it since, despite all the technological changes that have occurred in the meantime. To put this in additional perspective, consider that Apple issued the first-generation iPhone four years before the Security

## Related Content

For steps to take to minimize the risk of a ransomware attack and reduce the harm that a successful attack can cause, see

### RANSOMWARE PLANNING AND RESPONSE BEST PRACTICES

For an explanation of privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) impacting employers and the group health plans they sponsor, see

### HIPAA PRIVACY, SECURITY, BREACH NOTIFICATION, AND OTHER ADMINISTRATIVE SIMPLIFICATION RULES

For Practical Guidance resources addressing HIPAA, including detailed practice notes, checklists, templates, and specific clauses, see

### HIPAA RESOURCE KIT

For a discussion of enforcement of the privacy rule, Security Rule, Breach Notification Rule, and the transaction rule under HIPAA, see

### HIPAA ENFORCEMENT AND PENALTIES

For a collection of prominent recent guidance and enforcement actions undertaken by the Office of Civil Rights at the U.S. Department of Health and Human Services regarding HIPAA compliance, see

### HIPAA REGULATORY ENFORCEMENT TRACKER

7. U.S. Dept. of Health and Human Services, Office for Civil Rights, Fact Sheet: Ransomware and HIPAA (July 11, 2016). 8. 45 C.F.R. §§ 164.400–164.414. 9. 45 C.F.R. § 164.402. 10. *Id.* 11. 45 C.F.R. § 164.404(b). 12. 45 C.F.R. § 164.402.

13. 45 C.F.R. § 164.408(a). 14. 45 C.F.R. § 164.408(c). 15. 45 C.F.R. § 164.408(b). 16. U.S. Dept. of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. 17. U.S. Dept. of Health and Human Services, Office for Civil Rights, OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals (Aug. 16, 2016). 18. 45 C.F.R. § 164.406. 19. U.S. Dept. of Health and Human Services, Health Information Privacy, The Security Rule. 20. 45 C.F.R. §§ 164.306(e), 164.308(a)(1)(ii)(A), 164.316(b)(2)(iii).



Rule, and the iPhone is now into its 13th generation, while the Security Rule remains the same. The Security Rule framework has achieved its elasticity by focusing on what an entity must do without being very prescriptive about how things must be done.

The primary sources of the Security Rule's durability are its simplicity and uniformity.<sup>21</sup> Among other things, the Security Rule expressly incorporated a "flexibility of approach" that enables the same set of security considerations to be used for any sort of electronic health network.<sup>22</sup> Therefore, both a single provider medical practice and a multi-hospital system can—and must—apply the same Security Rule standards. Furthermore, although it was specifically built for the healthcare context, there is nothing unique about the Security Rule, which renders it useful for a variety of situations.

#### Elements of a Security Rule Risk Analysis

The core components of the Security Rule—administrative, physical, and technical safeguards—are as fundamental to the healthy operation of information systems as diet, sleep, and exercise are to personal health. In performing a Security Rule risk analysis, OCR recommends in a guidance document<sup>23</sup> that you consider the following factors:

- Knowing where your data lives
- Understanding and reasonably responding to anticipated risks
- Having plans for situations when things go wrong
- Ensuring that the policies and procedures supporting the risk analysis stay current

When done correctly, a Security Rule risk analysis should enable an entity's governing body to understand why its network is (relatively) safe. It will also enable the entity's information security team to understand how and why the network is (relatively) safe and, importantly, what needs to be done to keep it that way. Furthermore, if a ransomware attack does occur, having a current and comprehensive risk analysis will provide solid written evidence of an entity's compliance program. This is significant because OCR has stated,<sup>24</sup> as a general rule, that it does not impose sanctions on entities that have been reasonable in their compliance efforts: "OCR may decide not to investigate a case further if . . . [the] covered entity or business associate has taken steps to comply with the HIPAA Rules and OCR determines enforcement resources are better/more effectively deployed in other cases." In an effort to promote the use of recognized security practices, the so-called HIPAA Safe Harbor law requires OCR to consider an entity's use of such best practices in implementing any enforcement action.<sup>25</sup>

#### Updating Risk Analysis Documentation

One of the core aspects of the Security Rule risk analysis—the timing requirement for updates—is both a blessing and a curse. Specifically, the regulations require healthcare entities to review their risk analyses periodically and update as needed, but the regulations do not define either term or concept.<sup>26</sup>

On the blessing side, the lack of a prescriptive update period allows entities to reduce their administrative burden when there have been no significant changes to their systems. On the curse side, without

specific update requirements, entities frequently neglect their risk analyses such that they no longer reflect their current systems. This phenomenon was vividly revealed in 2020 by the OCR's publication of its 2016–2017 HIPAA audit results.<sup>27</sup> OCR found that only 14% of covered entities and 17% of business associates substantially fulfilled their Security Rule requirements. Among other things, the OCR audits concluded that entities generally failed to do the following:

- Identify and assess the risks to the ePHI in their possession
- Develop and implement policies and procedures for conducting a risk analysis
- Identify threats and vulnerabilities, consider their potential likelihoods and impacts, and rate their risks to ePHI
- Review and periodically update risk analyses in response to changes in the environment or operations, security incidents, or occurrence of a significant event
- Conduct risk analyses consistent with policies and procedures

Significantly, none of the above considerations are unique to health information; they apply to the business, operational, and human resources records of a healthcare entity as well. Furthermore, the above list reflects the minimum best practices that any entity in the modern economy should employ for its systems and data. In the healthcare context, HHS prepared a complete matrix identifying all required and suggested security specifications applicable to healthcare entities under the HIPAA Security Rule.<sup>28</sup> Entities of all sorts, including non-healthcare entities, should use it to evaluate

the nature, architecture, operations, and flaws in their information security systems.

In the absence of a defined periodic timing requirement, the sweet spot for ordinary updates to a risk analysis is probably in the 12-to-24-month range. Yet, it is important not to hold updates to a lockstep schedule. Instead, you should update your risk analysis (or at least relevant portions of it) anytime your entity has an actual or near-miss security incident and anytime your entity changes its physical footprint or its software or hardware structures.

#### Candor in the Risk Analysis

When engaging in a Security Rule risk analysis, you must be brutally honest with your client or organization. Self-deception can be fatal. The point of the risk analysis exercise is to consider critically each of the following:

- All the places in which data lives
- All the mechanisms and devices that enable access to that data
- All the ways that data flows from one place to another
- The manner in which that data is stored

#### Additional Best Practices Addressing Ransomware Attacks

In addition to employing the requirements of the HIPAA Security Rule risk analysis, as counsel to healthcare entities, you should also consider advising your clients or organizations to take the following actions to prepare for ransomware attacks or to mitigate their effects when they occur. Significantly, the overwhelming majority of action items below will also assist with generalized cybersecurity practices as well as improve the nondigital operations of an entity.

#### Contract for the Costs of Incident Response

Healthcare entities may include indemnification provisions in their HIPAA-compliant Business Associate Agreements (BAAs). These provisions typically cover situations in which a party breaches a term of the agreement. In doing so, however, the entities should ensure that the provision accounts for both breaches of the parties' agreement as well as breaches of PHI under HIPAA.

Indeed, a healthcare entity can be in full compliance with the HIPAA Security Rule but, nevertheless, experience a cyber incident that is no fault of its own. For example, the entity could experience an attack that is neither foreseeable nor preventable despite having a security infrastructure reasonable and consistent with industry best practices. In that case, although the attack would potentially be considered a breach under HIPAA, it might not constitute a breach of the parties' agreement. Accordingly, you should ensure that every BAA addresses the costs of incident response, particularly costs to comply with the HIPAA Breach Notification Rule, regardless of

<sup>21</sup> 45 C.F.R. § 164.306. <sup>22</sup> 45 C.F.R. § 164.306(b). <sup>23</sup> U.S. Dept. of Health and Human Services, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (July 14, 2010). <sup>24</sup> U.S. Dept. of Health and Human Services, *Health Information Privacy, Enforcement Data*. <sup>25</sup> Pub. L. No. 116-321, 134 Stat. 5072, § 1 (Jan. 5, 2021). <sup>26</sup> 45 C.F.R. § 164.316(b)(2)(iii).

<sup>27</sup> U.S. Dept. of Health and Human Services, Office for Civil Rights, *2016-2017 HIPAA Audits Industry Reports* (Dec 2020). <sup>28</sup> Published at 45 C.F.R. pt. 164 Appendix A to Subpart C.



the cause or culpability. In other words, healthcare entities should be sure to obtain reimbursement coverage for both contractual breaches and HIPAA breaches.

#### **Maintain Copies of Documents in Discrete Locations**

If all key contacts (e.g., lawyers, insurance companies, leadership, vendors, and clients) are maintained electronically, it may be very difficult, if not impossible, to collect necessary information swiftly during a ransomware attack. Therefore, you should consider maintaining paper versions of key documents.

In addition, and more realistically, an entity's leadership should keep certain digital records in personal email or distinct cloud storage locations to keep them immune from a system compromise. The key is to have another way to access vital information if the entity's systems are completely compromised. Not surprisingly, duplication of data and disaster operations preparedness are among the considerations under the Security Rule risk analysis framework.

#### **Use the News**

Rather than just take note of media reports of incidents that happen to others and move on, entities should appreciate that reported cases often provide glimpses of where cyber issues are heading. By paying attention to trends, entities can better prepare if they become victims of ransomware attacks. When your organization learns of an incident affecting another entity, a key reaction should be: "What if that had been us?" If your entity cannot answer that question, it could be a potential target.

#### **Invest in Cybersecurity**

Governing bodies may view cybersecurity expenditures as a significant waste of money, particularly since governing bodies may not appreciate the difference between attacks not happening and attacks being stopped. To those who do not understand the risk, the latter can feel like a nonevent. Indeed, many chief information officers can tell stories about their limited budgets, limited staff, and limited recognition. Things should not be this way.

An entity's governing body should be fully engaged in cybersecurity and supportive of efforts to keep systems secure. Among other things, this means that members of the governing body should understand that investing in cybersecurity is money well spent. You should consider periodically (e.g., annually) reviewing your comprehensive and updated HIPAA Security Rule risk analysis with your governing body to increase the chances that your organization will be willing to provide a sufficient budget to support appropriate security initiatives.

#### **Educate Your Organization**

To keep cybersecurity issues fresh and relevant, your entity's leadership should devote some modest amount of time to the topic at regular team and organizational meetings and via internal communications. Although your organization may believe that

annual security training sessions are sufficient to prepare for possible ransomware attacks, those sessions are likely little more than check-the-box compliance initiatives that probably are only minimally effective. To make best practices stick and to create an overall culture of security, workforce members need to hear repeatedly from their own colleagues about how the threats are real, how mistakes can happen, and how they can personally help keep the organization secure.

Accordingly, you should consider devoting five minutes of each internal meeting to cybersecurity topics. Additionally, your information security team should consider distributing periodic emails or other types of communications to your workforce highlighting cybersecurity topics or providing practical pointers.

#### **Customize Your Cybersecurity Plan**

Cybersecurity is not a one-size-fits-all affair, nor is it seamless and consistent. Furthermore, one-and-done training is unrealistic, as noted above. You should be prepared to make numerous updates to your entity's systems, to apply patches as they are released (and not when they are convenient), and to provide security training and announcements on the fly.

#### **Stress Compliance over Routine**

Entities should prepare themselves for some degree of pushback from employees when they are asked to change long-standing or cherished practices. Entities may need to remind their employees that security takes precedence over convenience and routine. Notably, your organization's leadership—who often are the targets of cyberattacks themselves—should not be immune from updated or modified security requirements.

#### **Support Internal Reporting of Concerns**

Human error is ubiquitous, and it is remarkable in its diversity. It is a fool's errand to think that human error can be prevented entirely. It can, however, be mitigated. While technical education and training regarding information security can help reduce the frequency of errors in the first place, maintaining a nonpunitive culture of incident reporting can help reduce the scope and severity of incidents overall. Indeed, an ideal security-supporting culture will provide routine training, welcome good-faith over-reporting of concerns, share the results of investigations, and make data security a point of organizational pride.

#### **Identify Legal Counsel in Your Insurance Policies**

It is increasingly common for cyber insurance policies to limit coverage to a certain list of panel attorneys. Although this can help ensure that the counsel involved with incident response is well-qualified, it often means that entities are forced to work with an entirely new legal team during an inherently challenging time. If you have an established legal relationship that you would like to use in the event of a data incident, be sure that your policy covers you when using your preferred counsel. This important coverage detail



should be negotiated as part of plan enrollment and renewal. Trying to negotiate choice of counsel while an incident is unfolding is likely to be both fruitless and a waste of already strained resources.

#### **Minimize Use of the Term Breach**

Because the word breach has a specialized meaning under HIPAA, entities should only invoke that term when they have completed the breach risk assessment process.<sup>29</sup> Until you determine a HIPAA breach has occurred, consider using alternative phrases such as data incident, security situation, or information event. Alternatively, consider qualifying your use of the term. For example, you may refer to an incident as a potential breach.

#### **Share Information with Others in Your Industry**

Keeping secrets about cyber incidents can facilitate subsequent attacks. To combat this, organizations exist to enable entities to share information with one another to collectively reduce risk. Consider joining your relevant information-sharing group to

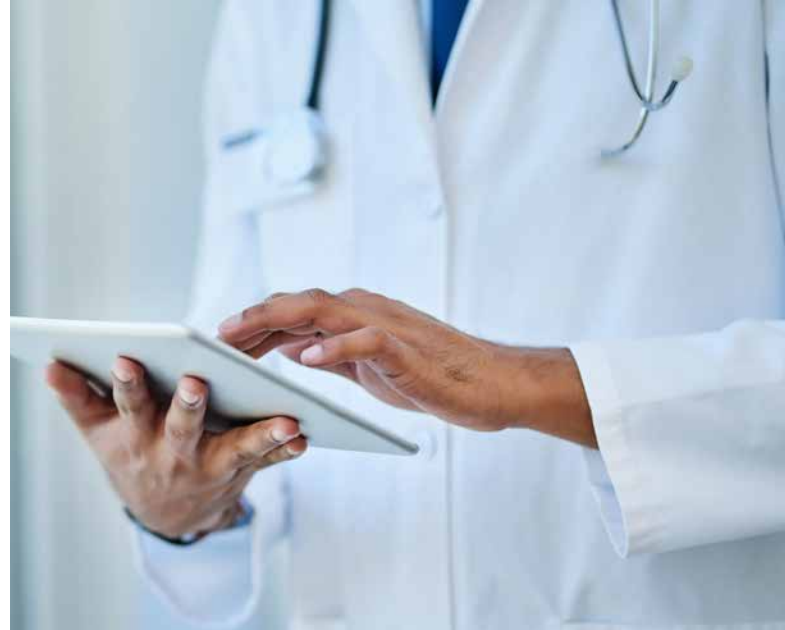
exchange information and learn from peers. For example, visit the Information Technology - Information Sharing and Analysis Center (IT-ISAC) site.<sup>30</sup>

#### **Review Government Guidance**

Ransomware significantly impacts the government given its effect on the economy. As a result, you should consider incorporating several government guidance documents into your incident response plan. At a minimum, if your entity has not already developed a response plan, you may choose to use these resources as references during a ransomware attack. Information is available from the following federal government agencies and departments:

- Cybersecurity and Infrastructure Security Agency<sup>31</sup>
- Federal Bureau of Investigation<sup>32</sup>
- U.S. Department of Health and Human Services<sup>33</sup>
- U.S. Secret Service<sup>34</sup>

29. 45 C.F.R. § 164.402. 30. <https://www.it-isac.org/>. 31. Stop Ransomware. 32. FBI, Scams and Safety: Ransomware. 33. U.S. Dept. of Health and Human Services, Office for Civil Rights, *Fact Sheet: Ransomware and HIPAA* (July 11, 2016). 34. U.S. Secret Service, *Preparing for a Cyber Incident*.



Eric B. Levine LINDABURY, MCCORMICK, ESTABROOK &amp; COOPER, P.C.

# Cybersecurity and Data Privacy in Commercial Real Estate

expenditures. Nonetheless, effective planning requires that your entity invest in cybersecurity. Therefore, if nothing else, the use of free resource checklists may be used to support capital expenditure requests to your entity's governing body.

## Conclusion—Living with the Ransomware Threat

Ransomware attacks are likely here to stay, and no one is immune. Entities can and should take various preventive and mitigating measures well before any event. Fortunately, one of the best tools for this exercise, the HIPAA Security Rule risk assessment, is required by law for both covered entities and business associates. Unfortunately, OCR's first audit suggests that the majority of these healthcare entities are not paying sufficient attention to information security. Putting aside the risk of enforcement penalties, failure to maintain a robust and current risk analysis likely will result in several significant lost opportunities and inherently greater susceptibility to a ransomware attack as well as other forms of cybersecurity incidents. In other words, ransomware issues should be treated as a chronic condition. **L**

*Nathan A. Kottkamp is a partner at Williams Mullen. He helps hospitals and health systems, academic medical centers, behavioral healthcare services providers, senior care providers and retirement communities, specialty physician practices, post-acute and long-term care providers, and others navigate federal and state healthcare regulations and contend with various operational challenges, including medical staff matters, ethics concerns, and complaint response.*

**RESEARCH PATH:** [Healthcare](#) > [Health Information Privacy and Security](#) > [Practice Notes](#)

## Take Advantage of Free Information

An overwhelming amount of no-cost information and tools exists to assist with cybersecurity, such as those from the government sources listed above. Additionally, numerous private consultants offer resources that may be used without purchasing any specific services. Of course, free does not mean cheap. To the contrary, entities should be aware that many free tools are very likely to recommend practices or initiatives that require significant capital

## Related Content

*For an example of a breach notice for a group health plan subject to HIPAA to notify affected individuals about an unauthorized use or disclosure of protected health information (PHI), see*

**HIPAA BREACH NOTICE (INDIVIDUAL)**

*For guidance in drafting a breach notice for a group health plan subject to HIPAA to notify prominent media outlets about an unauthorized use or disclosure of PHI, see*

**HIPAA BREACH NOTICE (MEDIA)**

*For a checklist that addresses items for covered entities and their business associates to consider in complying with HIPAA for PHI that is maintained or transmitted in electronic form, see*

**HIPAA SECURITY RULE EVALUATION CHECKLIST**

*For a sample policy for a group health plan to use to satisfy HIPAA privacy, security, and breach notification requirements, see*

**HIPAA PRIVACY AND SECURITY POLICY**

*For an overview of the legal rules and best practices for the disposal of PHI under HIPAA, see*

**DISPOSAL OF PROTECTED HEALTH INFORMATION UNDER HIPAA**

*For assistance in creating an agreement to require parties to comply with HIPAA, see*

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) CLAUSE**

*For a template of an agreement between an employer health plan and a third-party service provider that will handle PHI on its behalf, see*

**HIPAA BUSINESS ASSOCIATE AGREEMENT**

This article discusses several key considerations for evaluating cybersecurity and data privacy practices when counseling owners of commercial real estate (CRE).

#### THE ARTICLE ALSO DETAILS WHAT STEPS SHOULD BE

taken to mitigate the risk of unauthorized release or exposure of data in the possession of CRE owners. This article is written from the landlord's perspective and applies to all manner of commercial properties, including industrial, office, retail, healthcare, hotel, and mixed-use properties.

Understand that each class of commercial property is unique and comes with a distinct set of concerns, warranting site-specific counseling of CRE owners. Note as well that you must carefully evaluate the information in this article in light of all state and local laws applicable to your client's location. Finally, you should counsel your clients on their own internal cyber hygiene and security practices; it is just as important for commercial landlords to protect their own confidential data as it is for them to protect their tenants' data.

#### Getting Started – Client Information

As an initial step to counseling clients about the risks associated with cybersecurity/data privacy and CRE, it is important that you understand the level of sophistication of your clients, what type of properties your clients are leasing, and who their tenants are. This may appear to be elementary as most attorneys conduct client interviews when first engaged by any clients. But with CRE and cybersecurity, the conversation must go to a deeper level. Without this level of detail, it is possible that site-specific cybersecurity advice could be missed. This requires in-depth conversations with your clients to develop a thorough understanding of:

- The type of properties being leased
- The nature of the properties' usage
- The type of tenants utilizing the properties
- The services provided to the tenant by the owner/landlord of the properties

#### Type of Property and Tenant

Consider how different uses of CRE can impact legal issues when preparing your advice for a landlord client. For example, if your client leases an industrial warehouse that is climate-controlled—such as a warehouse storing perishable goods, pharmaceutical inventories, or cloud servers—and the climate controls are internet-accessible, the integrity of the HVAC system may be the single largest concern of the tenant and a particularly vulnerable access point for data intrusions. An outside threat actor accessing temperature controls of the warehouse and altering the pre-set climate conditions by just a few degrees could significantly damage the materials that are being warehoused or otherwise impair tenant operations.

Next, consider if your client owns a multi-tenant retail property, such as a mall, where the tenants may rely on an open (unsecured) Wi-Fi system that provides amenities and services to tenants and customers. Open Wi-Fi systems are convenient for customers but present a set of vulnerabilities that must be minimized. Imagine the business impact that could befall the tenants of this type of property should that open Wi-Fi system be used to infiltrate other building systems and cripple them.

Or, what if your client owns a smart building that integrates state-of-the-art building-management technologies to provide related benefits and building efficiencies to tenants, such as biometric recognition, inventory tracking technologies, and security and building systems (like elevators or lighting) that are monitored by a vendor at a centralized, off-site location? The breach of any of these systems could effectively shut down the building and impact the tenants' businesses. The resulting disputes that may arise between your client and its tenants are both foreseeable and preventable.

You need to recognize at the outset of client retention what your client's unique needs are related to the specific property, as there is no one-size-fits-all advice you can give to your client to achieve maximal protection from potential cybersecurity-related liability. For instance, the concerns of a hospitality-based piece of CRE like a hotel are far different than the concerns of an industrial property, so the lease provisions must be particularized to maximize the landlord's ability to maintain control.

You also need to learn about each property's operational technologies, meaning the software and hardware that monitor and control the property. Ask your client to describe what systems are used to control and monitor the properties. If more than one system has been installed, are they integrated, or do they function separate from one another? Are they internet-accessible?

Each type of property is associated with particular benefits and vulnerabilities requiring varying levels of landlord responsibility and protective measures. Today's tenants expect more amenities, modern systems, and seamless landlord-tenant interfaces as part of their leasing relationship. Furthermore, many commercial properties are supported by outside vendors such as HVAC service, plumbing, maintenance, and cleaning crews. As discussed in Evaluating Vendor Contracts and Security Measures below, tailoring your client's vendor agreements to address data privacy is an integral step in protecting your client from potential liability.

#### Single vs. Multi-tenant Properties

It is important to understand the physical layout and tenant composition of the property. Cybersecurity and data concerns



may be much less complex in a stand-alone, single-tenant property compared to a multi-tenanted office complex, apartment building, or retail property like a mall. For example, if your client is leasing a retail property, you need to determine who will be responsible for establishing infrastructure supporting a point-of-sale system. If a tenant's point-of-sale system connects to an external network, it will be more susceptible to attack. You need to address in the lease who is responsible for the maintaining the security and integrity of the connection to any external network.

Moreover, in a multi-tenanted property, landlords have to consider the implications of common areas such as lobbies, cafeterias, hallways, loading areas, garages, and restrooms. It is not uncommon for a multi-tenanted property to have sophisticated levels of security covering common areas and electronic security for off-hour access. A multi-tenanted property will also likely have a high number of vendors frequenting the property, engaged by either the landlord or the tenants. As the risk of cyber-intrusions increases, so does the complexity of the leases between your client and its tenants; the leases must address allocation of security responsibility for third parties, indemnification/hold harmless provisions, insurance

concerns, and mandated security efforts to be undertaken by tenants and their vendors. See Leasing—Allocating Responsibility to the Tenant through Lease Provisions below for more information.

#### Client's Experience and Level of Sophistication

You will need to consider the level of sophistication of your clients in order to determine how well-suited they are to addressing the risks of owning CRE in the digital age. It is not uncommon for CRE owners to be multigenerational owners who own properties for long periods of time. If this is the case, your client's properties and building systems may be outdated and in need of restoration, upgrading, and modernization to attract creditworthy tenants. But note that modernization is often accompanied by increased risks associated with building systems such as access management controllers, computerized air controllers and HVAC systems, cameras/security systems, and automated alarm/fire suppression systems. These types of systems require computer networks to operate, and many will also be connected to the internet to allow off-site monitoring, control, and troubleshooting. These connections are a popular attack vector for external threats. Your client must address potential risks by allocating liability in its leases and maintaining proper insurance.

## Questions to Ask Your Client

During your first consultation with your client, explore the following questions to better understand what sort of landlord you are counseling:

- How many properties do you own?
- Where is each property located?
- How long have you owned each property?
- What has the property been used for? Is the use industry-specific? For example, if it is a warehouse, what is stored there? If office space, what types of industries operate there? Is it retail, providing point of service terminals?
- How many tenants are in each property?
- If properties are vacant (partially or wholly), who/what is your preferred tenant for the vacant space?
- When was the last time the leases were reviewed by counsel?
- Are the properties managed by an independent, third-party property manager or by in-house staff? If by third parties, you should do the following:
  - Investigate the experience of the third-party vendors and review all property management contracts.
  - Ask when property management was last turned over to a new company.
  - Identify all internal employees with property-specific responsibilities and determine what information each has access to.
- Who is the landlord's support team? Be sure to obtain a list of all vendors and subcontractors that service the building, review all contracts, and maintain them in a centralized but protected location.
- Has the property been retrofitted or upgraded recently? If so, it is important to understand exactly what aspects were upgraded and who performed the upgrades. For security reasons, once a property that integrates technology accessible from outside the building (i.e., internet-accessible systems) has been built, owners should have all internet-accessible systems analyzed by an independent cybersecurity professional to ensure system integrity and change passwords and log-in information. This should not be done by the entity that performed the construction.
- What services or amenities are provided by the landlord to the tenants?
- Are the properties connected to the internet and, if so, are updated security measures in place (firewalls, virus protection, end-point security/encryption, malware)?
- How does each tenant pay rent (electronically or manually)?



- How does each tenant communicate with the landlord (email, text, phone)?
- What sort of tenant-based information and records does the landlord collect and why?
- Where does the landlord store property- and tenant-specific information (cloud servers, on-site network servers, tape backups, electronic spreadsheets, physical files)?
- How is property- and tenant-specific data protected from improper access and how is it purged? Be sure to review all document-retention and destruction policies.
- What sort of insurance policies are in place for each building?
- What experience does the landlord have with cybersecurity/data privacy in any context?
- Are there existing corporate cybersecurity/data privacy policies and training programs in place?

The questions are illustrative only and are not meant to be all inclusive. Only once you have a complete understanding of who your client is and their experience with their properties and tenants can you provide tailored advice. By asking these questions, you will also get the opportunity to educate your client, especially if your client is a first-time landlord or has limited experience in CRE.

### Risks to Consider

It is important to advise your clients of the data privacy-related risks associated with owning CRE. Historically, CRE has not been as focused on data privacy as other industries such as healthcare and manufacturing; CRE owners tended not to possess the same types of information and data as other industries that were more frequently targeted by outside threat actors. However, the risks of being targeted by cybercriminals is every bit as real for CRE owners and is growing with the advent of more CRE-friendly technology.

Do not assume that your client understands the nature of risks that a data breach can cause. And do not assume that because your client

owns a small number of properties or does not lease to national, big box clients that they will not be targeted by outside threat actors. You must explain to your clients that the following are some of the risks that they must address for each of their properties:

- **Safety concerns.** Consider how improper access to building systems, such as elevator, lighting, or air quality controls, could cause a safety risk to tenants.
- **Damage to tenant property, inventory, or productivity.** Understanding the nature of the business operating in your client's property is critical to assessing and controlling risk of damage to the tenant's business and the property's contents. We have already noted the potential impact on a tenant in a climate-controlled building storing temperature-sensitive products with an HVAC system that can be remotely accessed from outside the property. Should an unauthorized user access the HVAC system and raise the temperature a few degrees, it could be devastating to a tenant, who will then likely look to the landlord for compensation for any loss. Consider in the retail sector if a landlord loses control over building systems that force tenants to close their businesses pending recovery of the systems. Likewise, imagine the impact on tenant operations in a high-rise building complex if elevators and stairwell lighting are incapacitated for an extended period of time, forcing the closure of tenant offices on higher floors due to inaccessibility. These are the types of scenarios you need to review with your client.
- **Data breach liability/data exposure/data loss.** Your client needs to understand that if there is a data breach and your client maintained tenant data, anyone whose personal information is accessed could potentially sue the landlord. This means not just the tenants themselves, but the tenants' employees, their vendors, and even their customers and clients.
- **Loss of reputation and tenant trust.** CRE owners must understand that should a cyber-breach occur resulting in a disruption of operations or loss of data, inevitably tenants will look to the landlord for answers as to how such an incident occurred and whether it could have been prevented. The detrimental impact on a landlord's business could be severe. Reputational harm could follow the landlord for years, making them an unattractive landlord option to tenants.
- **Costs of data recovery and repairs.** Restoring data after exposure or a ransomware attack can be costly, especially if the data is not properly backed up. In some circumstances, your client may need to rebuild its entire computer system.
- **Litigation costs.** Last, but by no means least, are the costs of having to defend lawsuits brought by individuals and companies that have had their data accessed without authorization. These are the costs of defending any claims only and are exclusive of any damages or regulatory fines.



For instance, if your client performs an audit and the results show that no data-security policies exist or that any existing policies are outdated, your help may be needed in drafting or updating those policies. You can also assist your client by outlining the basic framework for this type of audit and advising your client to seek the assistance of an IT security professional in performing an audit.

In doing so and documenting your client's efforts, in addition to firming up the client's security infrastructure, you are creating a record of your client having taken reasonable measures to protect tenant information. The records of the audit provide a road map to a client for improving its data security, while providing a record of reasonable efforts that can be offered in defense of any claim asserted against a landlord for failing to take adequate measures to secure tenant information. Furthermore, your client may need to show that these efforts were taken in order to obtain cybersecurity insurance policies. Issuers of cyber insurance policies routinely demand that a potential insured complete questionnaires about data protection efforts undertaken by the potential insured.

With increased connectivity to cloud-based building systems, the Internet of Things, and remote-working employees, there are multiple points of access that can be exploited by hackers. It is now increasingly common that HVAC, electrical, lighting, security, safety, and building management systems can be accessed remotely in the ordinary course of building operations. It is crucial to understand how such systems are integrated into properties, what data they contain, and who can access them.

Locating and closing gaps in a client's IT systems require:

- Taking inventory of the systems integrated in the property
- Determining who is responsible for their maintenance (landlord or tenant)
- Documenting same in your client's lease
- Analyzing how these systems are configured for operations and remote access

You should advise your client to perform both physical and virtual inspections, including site walks and audits of contractors that completed work.

Ask your client what kind of tenant information is being stored and what is the purpose for having such information. For instance, if a tenant makes rental payments to a landlord electronically, it makes sense to have banking information of the tenant to effectuate payment. Also, consider advising your landlord client to get the express written consent of the tenant to obtain and store this information as part of the lease agreement. That way, your client has a record of having been authorized to store and use this data, which can bolster the defense of any claim raised by a tenant. Obtaining written authorization to store payment information is often overlooked in a lease, which normally contains rental terms such as the amount of rent, when rent is due, and late charge amounts.

### Location-Specific Data Concerns

Historically, local authorities and municipalities did not exercise control over the type of tenant data that a landlord may retain, but that practice is changing. It is important for you to evaluate all federal, state, and local laws related to data privacy in the jurisdiction of the property in order to fully understand your client's legal obligations and potential exposure.

A prime example of a local/municipal concern can be found in the New York Tenant Data Privacy Act (TDPA), established on May 8, 2021.<sup>1</sup> The first law of its kind in the United States, the TDPA addresses privacy issues related to the use of smart access systems in multifamily dwellings. Among other things, the TDPA requires that all owners of Class A multiple dwellings (a dwelling for three or more families living independently of one another used for permanent residential purposes) that use smart access systems (e.g., key cards, phone access, fingerprint) take the following steps:

- Provide tenants with a privacy notice written in plain language
- Obtain consent for the use of smart access systems
- Establish data retention periods for collected data
- Ensure that collected data is not sold or shared
- Create parameters surrounding the tracking of tenants
- Protect data that landlords collect

The TDPA provides for a private cause of action by a lawful occupant of a dwelling unit and allows of the collection of compensatory and punitive damages as well as counsel fees. Other states considering similar laws include Hawaii, Illinois, Maryland, Massachusetts, and Nevada.

Illinois already has the nation's most progressive laws on biometric data, the Illinois Biometric Information Privacy Act,<sup>2</sup> which establishes rules for collection of biometric data like fingerprints, facial features, and other physiological characteristics. California is also at the forefront of privacy issues, and your client will be subject to the California Consumer Privacy Act (CCPA),<sup>3</sup> if it collects consumer personal data, does business with any resident of California, and meets one or more of the following thresholds:

- Has annual gross revenues in excess of \$25 million
- Buys, receives, or sells the personal information of 50,000 or more consumers or households
- Earns more than half of its annual revenue from selling consumers' personal information

These laws provide examples of why determining the laws that apply to your client's operations is indispensable to your preparation of the lease of the property. If you do not understand what laws apply

to the property, it is likely that the lease you prepare will lack many necessary protections for your client.

### International Concerns

Another concern is whether your client is leasing property to individual international tenants, especially residents of the European Union (EU), or collecting data from such tenants. A landlord client may be subject to the General Data Protection Regulation (GDPR) without realizing it; even if your client is not leasing property to EU citizens or residents, it may still be collecting data from them simply by advertising properties online. If this is the case, a whole other set of requirements may apply to your client.

The GDPR protects citizens of EU countries, as well as noncitizens who reside in EU countries, and does not depend on the location of the entity holding those people's data. The GDPR is concerned with the following areas of data privacy, among many others:

- **Being informed.** A data collector must state why it is collecting personal information, how that information is used, how long it will be maintained, and if that information is intended to be shared.
- **Consent.** If your client is collecting information from international tenants, your client must obtain consent for the data collection.
- **Breach notification.** GDPR requirements for notification of a security breach are much more stringent than those of most U.S. states. For instance, EU residents must be notified within 72 hours of discovery of the security breach. Penalties for noncompliance under the GDPR are extremely severe, being composed of monetary penalties based off of worldwide sales figures.
- **Right to access.** EU residents have a right to obtain confirmation about whether and how their personal data is being processed.
- **Right to be forgotten or erased.** When data is no longer relevant to your client's original purpose, the provider of the information can request that their data be erased and no longer distributed.
- **Data portability.** EU residents have the right to obtain and reuse their personal data for their own purposes. Your client is responsible for creating processes and identifying employees who respond to requests for the portability or erasure of personal data.

Detailed analyses of individual jurisdictional laws such as the CCPA and the GDPR are beyond the scope of this article, but keep in mind that when you advise a CRE client, you must evaluate federal, state, and local laws, and possibly international law, related to property usage on an ongoing basis.

### Data Collection

Once you have educated yourself about your clients and discussed the list of potential risks with them, have your clients gather property-specific information in an effort to catalog any and all data that comes into their possession to determine what requires protection. This includes digital information as well as physical records, and records in your client's possession or in the possession of third-party vendors.

### Technology Audit

The first step for any commercial landlord is performing a technology audit to assist in understanding the threats their particular real estate and tenants present. An integral part of any competent cyber hygiene program is advising clients to perform a technology audit and to map their data. A technology audit is an evaluation of a business's information technology (IT) infrastructure and how the client currently uses that infrastructure, including a review of the client's operations and policies/procedures. A proper audit will show whether those operations and policies make the best use of the assets used by the organization and that the data that organization interacts with is stored in a secure manner. While the audit process is not a purely legal process that counsel performs for clients, it is beneficial for counsel to participate in the process and evaluate the results.

1. N.Y. City Admin. Code § 26-3001 et seq. 2. 740 ILCS 14/1 et seq. 3. Cal. Civ. Code § 1798.100 et seq.

It is imperative that you review each agreement with a vendor or other third party providing services to the property. This is especially true for any vendor that accesses any building systems digitally.

### Evaluating Vendor Contracts and Security Measures

Recall that the 2013 Target data breach was caused by a vendor of Target that accessed Target's systems to handle electronic billing, contract submission, and project management. Unbeknownst to the vendor and Target, the vendor had been the victim of a sophisticated cyberattack that infected the vendor's systems with malware. The resulting data breach cost Target millions of dollars and significantly damaged its reputation and brand.

You should draft a vendor-management policy for your client that can also become a tenant obligation under a lease. The goal of this policy is to ensure that your client performs proper due diligence when hiring vendors that will have access to the landlord's computer network and integrated building systems, as well as mandating compliance with any applicable data privacy and security laws. The policy should also:

- Delineate your client's oversight of the vendor and testing of services it provides
- Outline exactly what information is being utilized by the vendor
- Mandate that the vendor provide copies of its own security policies and controls to your client as part of the engagement process

It is important for your client to interface with vendors to determine how vendors are using the landlord's data and what steps are being taken to protect it.

It is imperative that you review each agreement with a vendor or other third party providing services to the property. This is especially true for any vendor that accesses any building systems digitally. You should focus on the following areas:

- **Indemnification, defense, and hold harmless provisions.** Any vendor that has access, or even potential access, to your client's IT systems and data must agree to indemnify, defend, and hold the landlord harmless from any data breach arising from the vendor's failure to secure data. Such indemnity language must be broad and not limit the amount of liability. Your client should be indemnified, defended, and held harmless from losses of all types, including third-party damages, regulatory fines, counsel fees, and costs of litigation. Be sure to include language obligating

the tenant to defend, not just indemnify and hold harmless, your client.

- **Limited access to data and critical systems.** The vendor agreement should include a provision limiting access to your client's critical systems and information to as narrow a field of persons employed by the vendor as possible. By limiting the number of persons who can access the property and its systems, you restrict access to confidential information only to persons who need the information to perform their jobs.
- **Notice of breach requirements.** The vendor agreements should include language requiring any vendor or third party servicing the property to provide immediate written notice to your client should the vendor become aware that it has or may have been the victim of a cyber-breach.
- **Scope of work and systems accessed.** Vendor agreements should clearly define the exact scope of work to be performed and the building systems that need to be accessed in order to perform the work. This list should in turn be reviewed with your client's IT team and its IT security professionals to identify areas of concern, gaps in protection, and efforts that need to be added to the scope to ensure system integrity.
- **Representations and warranties about the vendor's security program/practices.** It is important that any vendor agreement contain detailed representations and warranties of the vendor outlining that vendor's data-protection efforts. For instance, a landlord needs to know that its vendors engage in their own data-security practices at a level of sophistication at least equal to the landlord's. If not, this could cause a number of problems, including a disparity in security efforts that increases the risk of liability. Additionally, your client's insurance carrier may require that all third parties engaged in business with your client show proof of adequate security measures as a condition of obtaining insurance coverage. Engaging a vendor who fails to meet this standard could result in a denial of issuance of a cybersecurity insurance policy. While it is not common to include a representation or warranty about prior cyber incidents in a vendor agreement, you should ask the vendor if it has been involved in any previous data breach/cybersecurity incident.

- **Limitations of liabilities.** Be careful to evaluate vendors' limitations of liability. It is not uncommon for a vendor to attempt to limit its liability to the value of its contracted services and limit liability for, or refuse to cover at all, consequential or punitive damages. Remember that the potential liability for a cyber-breach can be extensive based on how improperly accessed data is used, sold, and exposed. With virtually unlimited exposure possible, it behooves a landlord to negotiate hard against any limits of liability for cyber-breaches.
- **Insurance provisions.** You need to pay attention to what manner of insurance and coverage limits a vendor has obtained to determine if it provides adequate coverage for your client. You should insist on reviewing copies of the vendor's cybersecurity insurance policies and require that your client be named as an additional insured. (Remember that a cyber insurance policy provides different coverage than a general liability policy, which provides coverage for bodily injury and damage to property resulting from the operations and services provided by the covered entity.)
- **Dispute resolution, choice of law, and venue.** As with other contracts you review with your clients, make sure that the vendor's dispute provisions, choice of law, and venue selection provisions are consistent with your client's expectations.

### Security Testing and Incident Response Plans

One of the most important things you can counsel your client on is to regularly conduct investigations to understand the current state of its cybersecurity defense weaknesses and vulnerabilities. This practice includes periodically performing vulnerability assessments (hiring an IT security professional to identify, quantify, and prioritize the vulnerabilities in a system) and penetration testing (performing an authorized simulated cyberattack on a computer system using a third party commonly known as an ethical hacker to evaluate the security of the system). These technical exercises should become part of your client's standard business operations as they are crucial for maintaining good cyber hygiene.

### Attorney-Client Privilege and Work Product Doctrine

Your client's investigations will likely produce an extensive list of potential problem areas that, in a perfect world, would all be promptly and exhaustively remedied. In reality, this remedial approach is often not feasible as most companies have budgetary and other practical limitations that may require them to prioritize which vulnerabilities to address first, and the degree of remediation they can reasonably undertake.

This means that it is possible that a breach could affect your client's tenant before all of the identified vulnerabilities are remedied. Imagine if your client is sued for such a breach and you had to disclose the results of a vulnerability assessment when the recommended solutions have not been completed. If your client

### Related Content

*For guidance on managing the work flow for purchasing and selling commercial real estate, including detailed practice notes, templates, and checklists, see*



*For a collection of retail leasing resources, including letters of intent, lease agreements, work letter agreements, lease guaranties, and ancillary retail lease agreements, see*



*For a discussion of key industrial lease provisions and practical tips for drafting and negotiating an industrial lease from the landlord's or the tenant's perspective, see*



*For information on the office leasing process and where to find Practical Guidance practice notes, templates, checklists, and clauses related to office leasing, see*



*For an overview of data privacy and cybersecurity issues that companies typically address regarding COVID-19, see*



experiences a cyber-breach incident, this written report is likely to become a prominent exhibit of any plaintiff action against the company over that breach. After all, the investigative results will show that your client knew about certain vulnerabilities and chose not to remedy several of them at that time.

If done properly, your involvement in the process can allow your client to rely on attorney-client privilege and/or the work product doctrine to maintain the confidentiality of the investigative results. The overriding principle of using privilege is straightforward: to protect your company's breach response efforts from usage by third parties or regulatory agencies in litigation arising from a breach. Attorney-client privilege protects confidential communications between attorneys and clients over the course of a professional relationship from discovery by adverse third parties. The work product doctrine protects from disclosure those documents and other tangible things that a party or a party's representative prepares in anticipation of litigation. You must understand the difference between the privileges and also recognize that privilege applies

differently if you are in-house counsel to a CRE client or if you are outside counsel engaged by a CRE client.

You should research the requirements of the jurisdiction in which you are practicing to ensure that you satisfy all of the elements required to invoke attorney-client privilege. Recognize that the work product doctrine may not apply unless you are taking steps in anticipation of specific litigation. At a minimum, when engaging a vendor to perform a vulnerability assessment, you should:

- Require all vendor contracts to be signed by counsel
- Instruct the vendor to present all reports to you and not directly to the client
- Ensure that all directions and communications, other than those related to logistics and scheduling, go through counsel and the vendor
- Delineate the payment responsibilities of the client and your office, being careful to follow governing case law on how the payment of fees will affect the privilege

Make clear that the purpose of engaging this vendor is to:

- Analyze the client's potential exposure to liability and regulatory compliance
- Enable you to prepare the client to defend against any litigation arising from the use of the client's computer network and data it contains
- Allow you to provide guidance on complying with any and all applicable laws

### In-House Counsel Concerns

Companies with their own in-house counsel may sometimes want to avoid the additional expense of hiring outside counsel to arrange the cybersecurity vulnerability investigation. By having in-house counsel undertake the arrangements, however, a company may risk losing attorney-client privilege.

In-house counsel tend to have dual roles at their companies, meaning that they frequently provide both general business advice and legal advice. It may therefore be more difficult for a client to prove that in-house counsel was truly retaining the cybersecurity vendor for the purpose of providing legal advice, rather than simply as part of the in-counsel's general business role at the company or as an officer of the company.

Outside counsel, on the other hand, tend to be brought in specifically for the purpose of providing legal advice on a focused issue, and therefore the potential dual role issues that in-house counsel may face can be avoided.

For their own protection, in-house counsel should instruct outside counsel to make all arrangements necessary to engage the IT security vendor who will perform cybersecurity vulnerability assessments. If these vulnerability assessments are undertaken at the direction of an attorney for the purpose of providing legal advice to the attorney's client, then arguably the report detailing the client's cybersecurity weaknesses will be protected from disclosure under attorney-client privilege. This can allow the client to be comfortable in doing the right thing by having its cybersecurity program

evaluated and improved, while potentially avoiding having a list of vulnerabilities turned over in a future plaintiff litigation.

In-house counsel should work closely with management at their company to evaluate when it is appropriate to bring in outside counsel in connection with a cybersecurity vulnerability investigation and potentially obtain the benefits of attorney-client privilege for the results of that investigation.

### Leasing—Allocating Responsibility to the Tenant through Lease Provisions

You will need to work with your landlord client to allocate responsibility for technology system integrity to their tenants through lease provisions. These provisions must clearly define each party's role and responsibilities in the security process. These responsibilities will be ongoing throughout the lease term and should be thoroughly and clearly delineated.

Topics that must be addressed during lease negotiations include the following:

- **Allocating technology-related fit-up, upgrade, and repair responsibilities between landlord and tenants.** In any landlord work letter, it is important to be explicit on the limits of any work done by the landlord, including stating clearly what ongoing obligations, if any, the landlord retains for maintaining the security of any fit-up work. For improvements/fit-up work done by tenants that are integrated into the building systems, you need to include a provision giving the landlord the right to evaluate and approve such work to ensure that the integration is successful and secure, while at the same time mandating that ongoing maintenance and monitoring for security remain with the tenant.
- **Representations and warranties as to the condition of the property.** You should be sure that the lease references the current condition of any cybersecurity/data-related infrastructure of the property. It may be that tenants do not normally inspect certain building aspects such as Wi-Fi hubs, fiber-optic connections, or internet connections available on the property, but allowing them to do so can serve as a basis to argue for an allocation of liability should a breach occur in a system that a tenant could have inspected but chose not to.
- **Capping/limiting damages for cyber-related losses.** Be careful to draft broad language when describing the limitations on the damages a tenant is waiving. If possible, negotiate a finite damage cap, in addition to narrowing the types of damages for which your client must reimburse a tenant. However, you should expect a tenant to demand that any limitation on damages to which it is subject to mirrors the limits of liability that your client is demanding.
- **Indemnification, defense, and hold harmless provisions.** Similar to the indemnity provision discussed earlier related to vendors, you should negotiate a lease provision requiring the tenant to

indemnify, defend, and hold the landlord harmless from any data breach arising from the tenant's failure to secure its computer systems and data. This indemnity language must be broad and not limit the amount of liability. Your client should be indemnified from all types of losses, including third-party damages, regulatory fines, counsel fees, and costs of litigation arising from a tenant's data breach. This is especially important in multi-tenanted properties.

- **Cyber-related insurance concerns.** You should draft the insurance provision to mandate that all tenants obtain separate cyber insurance policies naming the landlord as an additional insured so that there is coverage for any breach caused by a tenant's negligence. This is especially useful in multi-tenanted properties, like retail and office buildings. If you wish to mandate specific policy limits, you will need to consult with your client and an experienced cyber insurance broker to estimate potential breach-related costs in order to calculate acceptable limits.
- **Notice requirements should tenant learn of a cyber-breach.** It is critical for a tenant to provide notice to a landlord of any potential cybersecurity breach as soon as possible. The ability to minimize the negative impact of any breach weakens the more time passes from the time of the breach.
- **Consent provision from tenants for collecting and use of information.** You should include language in the lease expressly having the tenant authorize the landlord to collect, maintain, and use information collected.
- **Landlord's approval of vendors used by tenant for fit-up, repairs, and modernization.** You should include a provision in the lease requiring the tenant to obtain the landlord's approval of any vendor that will be accessing any building systems or potentially coming into contact with any information maintained by the landlord. The landlord's approval of the vendor should not be unreasonably withheld, but by requiring the landlord to approve the vendors accessing building systems, your client will be able to procure first-hand information about third parties entering into its property and manipulating the building systems and keep itself updated on any modifications and service to the building systems.

### Security Policies and Procedures

Part of your duty as counsel to a landlord is to help your client develop a robust and comprehensive security practice, including protocols and policies that must be followed pertaining to cybersecurity. These policies provide a road map for your client's organization to follow. It may also be required in order to obtain cyber insurance coverage. Like other enterprise-level policies (such as employment and facilities policies), these policies should be reviewed annually and provided to all employees of your client. The following policies should be drafted:



■ **Remote access and teleworking policy.** Due to the rise in remote working, a remote working policy is indispensable. Drafting a comprehensive written remote access policy enhances the likelihood that everyone will act uniformly and follow the same processes. The policy will need to address:

- Eligibility for remote access
- Procedures for obtaining permission to work remotely
- What technology will be used in implementing the access
- Protocols for transmitting confidential information
- What discipline may be imposed for noncompliance

■ **Cyber incident response plan.** Your client will need to draft a systematic incident response plan that provides a detailed process to follow in the event of a cyber incident. This plan should:

- Identify the response team
- Define responsibilities for members of the team
- Set forth exact procedures for responding to a cyber incident
- Outline how to collect information to respond to an incident
- Provide evidence preservation protocols
- Establish proper channels of communication within the landlord's company

■ **Employee training policy.** As discussed below in Education and Monitoring, your client should engage in periodic training of its employees to reinforce the need to secure data and to instill best practices among its personnel. All employees, without exception, should participate in the training and your client should maintain records of completion. Training should cover all aspects of data protection, including:

- File maintenance
- Email protection
- Password management
- Acceptable transmission of data internally and externally
- Use of approval technologies such as multifactor authentication and verification of authority before releasing data

■ **Computer privacy policy.** Your client should draft and disseminate a policy advising that all computers are company property and there is no right to privacy for the information they contain. The policy should also advise that your client reserves the right to monitor and record all activity on their computer systems.

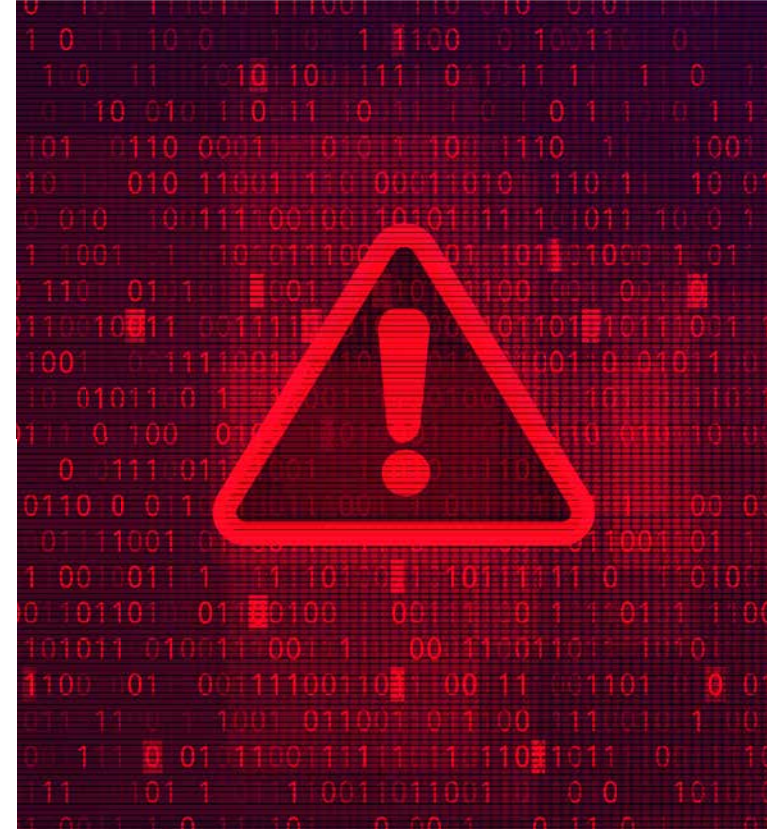
## Insurance Concerns

You should discuss the need for your client to insure cyber-risks as part of its overall insurance program. As noted earlier, cyber

insurance is unique and the risks it covers are distinct from the protections provided by a commercial general liability policy. Cyber insurance can improve your client's cybersecurity program by requiring your client to engage in the application process, which forces it to evaluate its capabilities and weaknesses. It is also beneficial in the event of a cybersecurity breach since it provides a funding source for recovery of losses and assists your client resume normal operations.

Depending on the type of properties owned by your client, they will need distinct types of coverage as well as differing policy limits of coverage. Your role as counsel to a CRE landlord is to engage in the process and work with your client and an experienced cyber insurance broker to obtain coverage. The following types of coverage should be considered:

- **Network security coverage.** This insures first-party costs arising from a cyber incident, including the cost of:
  - Breach notification
  - Data restoration
  - Legal expenses
  - Public relations
  - Ransomware
  - Identify theft restoration
  - IT forensics
- **Privacy coverage.** This insures third-party costs associated with the release of sensitive information of third parties, like tenants and their customers. It includes violations of privacy-related laws.
- **Business interruption coverage.** This insures for stoppages and interruptions of your client's operations due to a cyber incident including losses arising from systems failures.
- **Errors and omissions coverage.** This insures for allegations of negligence, omissions, or breaches of contract when a cyber incident prevents your client from delivering services to its tenants.
- **Social engineering coverage/theft and fraud coverage.** This is insurance designed to protect your client from being victimized by email/phishing schemes, such as fraudulent wire transfer situations.
- **Reputational harm coverage.** This coverage gives your client the ability to address potential harm to its brand/reputation arising from a cyber incident.
- **Data restoration coverage.** This insures the costs of restoring your client's data that was lost or damaged due to a cyber incident.



## Responding to Data Breaches

Should your client ever be the victim of a cyber-breach, your role as counsel during that crisis is critical. Presumably, you will be the first person that your client calls for advice. Moreover, your assistance in the response may afford your client the protection of attorney-client privilege, as discussed above.

If your client has a cyber insurance policy, you need to ensure that your client immediately contacts its insurance carrier. Depending on the type of data breach (e.g., ransom attack/system lockout vs. unauthorized access), the insurance carrier may assume the breach response. If coverage is available and the insurance carrier assumes the response, then step aside to assure that the insurance carrier has no basis to deny coverage.

If your client does not have cyber insurance coverage or if for some reason the cyber insurance carrier does not otherwise respond to the breach, then it is your role to either manage the breach response or engage counsel with expertise in breach response. As with vulnerability assessments and penetration testing, having counsel manage the breach response may allow your client to argue that the breach response is subject to attorney-client privilege. You must engage a vendor experienced in cyber-breach responses immediately, being sure to preserve any and all evidence of the breach for analysis and remediation. You will also need to engage a computer forensic vendor to diagnose the breach and to contain the problem. This should be done without delay and through counsel's engagement, again to invoke privilege to protect the results of any analysis undertaken.

Once the breach is contained, you should meet with your client to review the findings of the vendor that performed the breach

response to ensure proper implementation of any remedial measures, and to follow recommendations putting into motion further steps to protect against litigation, such as:

- Issuing any proper breach notices to affected persons under the appropriate state laws
- Responding to any regulatory requirements
- Notifying insurance carriers
- Identifying witnesses and documents to be used at trial

## Internal Threats and Securing Your Client's Data

You must guide your client on combating cyber-threats and protecting data internally. If there is one department in every company that has in its possession of a literal treasure trove of sensitive information, it is the human resource department, which maintains employees' names, addresses, dates of birth, Social Security numbers, bank account information (for direct depositing of paychecks), health and medical information (originating form health insurance applications, flex plan reimbursement materials), and financial information, especially if your client has a self-directed 401(k) plan and contributions are automatically deducted from payroll. A data breach implicating your client's human resources department could be devastating.

### Related Content

For assistance in drafting a commercial real estate leasing agreement to document terms regarding the proposed lease of space in an office building, see

 [OFFICE LEASE AGREEMENT](#)

For an example of an agreement for the lease of retail space in a mixed-use building, shopping center, or stand-alone property, see

 [RETAIL LEASE AGREEMENT \(LONG FORM\)](#)

For a sample commercial and industrial lease agreement, with detailed practical guidance and drafting notes, see

 [COMMERCIAL AND INDUSTRIAL LEASE](#)

For an explanation of the types of risks to an enterprise that may be covered by cybersecurity insurance, see

 [CYBERSECURITY INSURANCE](#)

For more information on the common varieties of business insurance, see

 [BUSINESS INSURANCE BASICS](#)





In order to know how to protect employee data, your client must be counseled on understanding what data they have in their possession and where the weaknesses are in their data maintenance. This is similar to the evaluation of your client's tenant data discussed above. You should advise your client that its human resource department directors should meet with their IT counterparts to ensure that they have an understanding of the various data privacy threats they face. You must advise your client that it should adopt the principle of least privilege, which means limiting access rights of employees to the minimum permission they need to perform their job duties. For example, if a staff member is responsible solely for processing, that individual should not be given access or rights to health insurance records.

### Education and Monitoring

Counsel your client on the need to ensure that employee training is undertaken on a regular basis and includes topics such as:

- Securing mobile devices
- Data safeguards for remote employees
- Password protection
- Recognizing common cyber-threats like social engineering, phishing, and ransomware

Make all training mandatory and ensure that proof of attendance becomes part of an employee's personnel file. Doing so will insure employee education is current, while also creating a record of reasonable training to be used as business records evidence to support any defense to litigation a company may be subjected to in the aftermath of a cyber-breach. Maintaining such records may also be a condition of a cyber insurance policy maintained by a company.

Also consider advising your client to monitor employees' computer usage to detect employees accessing documents that they are not

supposed to or unusual downloading activity. Ensure that your client has a computer privacy policy in place that advises employees that they are subject to monitoring and have no expectation of privacy in their work devices. Doing so is a legal requirement but can also act as a deterrent for some employees who will limit their online usage for fear of employer access to their browser history. This in turn reduces the chances of employees accessing suspicious websites at work.

Counsel your client to commence data privacy training during the onboarding process by providing all data privacy policies and procedures during any orientation or training for new employees. It is important to encourage employees from their first day of employment to understand that timely notice of any possible data breach is crucial and that, while all data privacy events must be reported, innocent mistakes happen. While employees can be disciplined for breaches of data privacy protocols, advise your client that it is important to foster an environment where employees feel free to report problems and are not in fear of retribution for reporting.

Finally, you should counsel your client to be vigilant and keep watch for rogue employees—those individuals who are dissatisfied with work and may be prone to destroying materials or taking sensitive materials with them should they leave the company, or worse, those who may affirmatively try to hurt a company through the release of sensitive information. **L**

**Eric B. Levine** is President of Lindabury, McCormick, Estabrook & Cooper, P.C and a member of the firm's Executive Committee. Eric concentrates his practice in commercial, probate, and general litigation. His trial and dispute resolution experience encompasses a wide variety of matters, including cybersecurity & data privacy, insurance defense and coverage, contract matters, commercial real estate, and construction litigation matters. Mr. Levine is co-chair of Lindabury's Cybersecurity and Data Privacy practice and assists businesses in the creation of their internal cyber-breach response team. He advises corporations and their executives on mitigating the impact of cyber-breaches and counsels on the regulatory reporting and client/customer notification responsibilities after breaches occur. An accomplished litigator with trial experience in both state and federal courts, Eric works with corporations to defend cyber-related claims.



RESEARCH PATH: [Real Estate](#) > [Commercial Purchase and Sales](#) > [Practice Notes](#)

Timothy Murray MURRAY, HOGUE & LANNIS

## Rules, Rules, Rules . . . Contract Law Is Awash in Rules (That Too Many Attorneys Don't Know)

I was asked by a company to revise its standard boilerplate legal terms found on the back of its purchase order form so that its terms would prevail in a battle of the forms contest—where contracts are formed by parties exchanging documents without signing off on the same piece of paper. Proper drafting can enhance the chances that the terms will be construed as the contract in such a battle.

I IMPROVED THE FORM, AND MONTHS LATER, I FOUND myself in the office of the company's head of procurement. I asked if he had received any feedback on the new form.

"We really appreciate what you did for us with that new form," he gushed, to my delight. It is not often that a client is so appreciative.

But then he pointed to a large box on the floor. "As soon as we use up that box of old forms, we're going to roll out your new ones."

It wasn't so funny at the time. That failure wasn't my fault. This article is about failures that are the attorney's fault—and how to avoid them.

Professor Arthur Corbin, who wrote the most influential legal treatise America has produced, *Corbin on Contracts*, preached that contract law is constantly evolving just as society constantly changes (or, depending on your perspective, spins out of control). This view hasn't always been universally accepted. Corbin reported that by the time he and the other great contract law treatise writer, Samuel Williston, worked together on the first Restatement of Contracts, "Williston had virtually ceased to read recent cases."<sup>1</sup> Williston was the product of the late 19th century



Harvard Law School faculty "that convinced its students that it had arrived at final principles."<sup>2</sup>

1. William Twining, "Looking Back Will Still Keep Us Looking Forward": A Letter from Arthur Corbin to Soia Mentschikoff upon the Death of Karl Llewellyn, 27 Yale J.L. & Human. 201, 203, n.9 (2015) (citing Arthur L. Corbin, Answers to Questions 7 (Oct. 1965) (unpublished typescript) (on file with author of the article)). 2. *Id.*

Of course, there are no final principles, but sadly, we all know practitioners with a final principles mindset—self-identifying experts in contract law who aren't especially interested in what the courts have said about contracts recently.

The courts tell us how to draft, and we ignore the judicial precedents at our peril. Contract law is encrusted with rules—the rules differ from place to place, and they change over time. We can't have confidence that we've drafted an effective contract without a thorough understanding of the daunting complexities of contract law. Most contract cases are lost, won, or better yet, avoided altogether before the document is even signed—in the drafting stage.

To assist attorneys who draft contracts, my *Corbin on Contracts* co-author Jon Hogue and I have written a new volume called *Corbin on Contract Drafting*, to be published in the fall of 2022. It explains why contracts have to be drafted in certain ways—the why is most of the book. It's not a book about drafting style, and it isn't a formbook. It's a book forged in the fires of messy, mystifying, real-world cases. This short article is a sampling—the tip of the iceberg—of just a few of the areas we cover.

### Whose Rules Apply?

There is not one, monolithic contract law. Figuring out which rules apply is its own challenge. The rules differ from state to state. For example, many states say that in determining whether a contract is integrated, extrinsic evidence is admissible, but many others disagree.<sup>3</sup> Many states say that a time is of the essence clause in the contract is conclusive<sup>4</sup>—late performance means that the breach is material and the non-breaching party's duties are discharged. But other courts say that a time is of the essence clause is not conclusive.<sup>5</sup> For the dreaded battle of the forms, many states apply the knockout rule,<sup>6</sup> but some major states—including California<sup>7</sup> and apparently New York<sup>8</sup>—do not.

It matters if the predominant purpose of the contract is for goods or services.<sup>9</sup> If for goods, the Uniform Commercial Code (U.C.C.) applies (the seller's obligations are measured by the perfect tender rule); if for services, the common law applies (the seller's obligations are measured by substantial performance). For sale of goods contracts made by parties whose principal places of business are in different countries

that abide by United Nations Convention on Contracts for the International Sale of Goods (CISG),<sup>10</sup> the CISG applies (unlike U.S. law, it has no parol evidence rule). Parties can opt out of the CISG in their choice of law provision, but most courts say that a generic choice of law clause specifying, for example, that the laws of the state of New York apply is not enough since CISG is, itself, part of the law of New York. The clause has to say that the parties opt out of CISG.<sup>11</sup>

Figuring out which law applies can be akin to a game of whack-a-mole. Try to follow the bouncing ball in the following case. Wadley Crushed Stone Company wanted to build a granite plant in Alabama that would process 500 tons of granite per hour. It signed a contract in Georgia to buy equipment from 1st Quality Equipment Company. The contract also said that 1st Quality would provide “erection, installation, and electrical” services. 1st Quality supplied the equipment, but Wadley refused to pay for some of it because it did not meet the 500 ton-per-hour requirement. Five years after the plant was completed, Wadley sued 1st Quality. The court sat in Alabama, so it applied Alabama choice of law rules. Since the contract was signed in Georgia, Georgia law governed the substantive claims. But Alabama considers the statute of limitations to be a procedural matter (as most states do), so the court applied Alabama law to determine whether the claim was time-barred. The case hinged on whether the contract was one for goods or services. If for goods, the action was untimely because the U.C.C. has a four-year statute of limitations.<sup>12</sup> If for services, Alabama's six-year statute of limitations<sup>13</sup> would allow the claim. Since the court applied Georgia law to interpret the contract—even though this issue related to the statute of limitations—Georgia law, not Alabama law, applied to decide whether the contract was for goods or services. To determine whether the four-year U.C.C. or the six-year non-sale of goods statute of limitations applied, the court applied Georgia's predominant factor test and concluded that since over 95% of the contract was for goods, “it seems pretty clear under Georgia case law . . . that the contract is for goods and not services.” The breach of contract claim was time-barred.<sup>14</sup>

The difference in state laws is dramatically illustrated by restrictive employment covenants that are drafted too broadly. There are three principal approaches courts take with respect



to this issue,<sup>15</sup> each offering far different outcomes and suggesting different approaches in drafting:

- The strict blue-pencil approach: If the unreasonable portion can be cleanly excised with a proverbial blue pencil while the remaining words constitute a complete and valid contract, the restrictive covenant can be enforced (without the excised words).<sup>16</sup> Under this approach, “[c]ourts cannot revise, rearrange, or add language to the agreement between the employer and employee,”<sup>17</sup> they can only cross out. This approach incentivizes employers to draft to the limit of reasonableness—to word the clause as broadly as possible while making sure that a stand-alone part of it is reasonable in case it is challenged. (The problem is, most employees do not challenge them.) So, if a restrictive covenant forbids an employee from competing “in the city

of Philadelphia and in the Western Hemisphere,” and if the “Western Hemisphere” portion is unreasonable but “Philadelphia” is reasonable, “Western Hemisphere” can be excised while “Philadelphia” is retained.

- The liberal blue-pencil approach allows a court flexibility to modify an unreasonable provision in any reasonable way. So, if a covenant forbids competition in Pennsylvania, but only Philadelphia is reasonable, the clause will be limited to Philadelphia only. Reformation is not allowed if the covenant was included in bad faith or if it was blatantly unreasonable when drafted.<sup>18</sup>
- The all or nothing approach—either the clause is reasonable, or it isn't. If not, it will not be enforced. There are drawbacks associated with this approach, but it incentivizes employers to draft reasonable provisions.<sup>19</sup>

3. Gregory Klass, *Parol Evidence Rules and the Mechanics of Choice*, 20 *Theoretical Inq. L.* 457, 470-471 (2019). 4. E.g., *Greenland Super Mkt., Inc. v. KL Vegas, LLC*, 2019 Nev. Unpub. LEXIS 1271, 452 P.3d 411 (Nov. 21, 2019). 5. E.g., *Kodak Graphic Communs. Can. Co. v. E.I. du Pont de Nemours and Company*, 2015 U.S. Dist. LEXIS 834 (W.D.N.Y. Jan. 6, 2015), *aff'd*, *Kodak Graphic Communs. Can. Co. v. E.I. du Pont de Nemours & Co.*, 640 Fed. Appx 36 (2d Cir. 2016). 6. See *General Steel Corp. v. Collins*, 196 S.W.3d 18 (Ky. Ct. App. 2006); *Power Paragon, Inc. v. Precision Tech. USA, Inc.*, 2009 U.S. Dist. LEXIS 21363 (W.D. Va. Mar. 17, 2009); *Flender Corp. v. Tippins Int'l, Inc.*, 2003 PA Super. 300, 830 A.2d 1279 (2003). 7. *Steiner v. Mobil Oil Corp.*, 20 Cal. 3d 90, 569 P.2d 751, 141 Cal. Rptr. 157 (1977). 8. E.g., *Movado Group, Inc. v. Mozaffarian*, 92 A.D.3d 431, 938 N.Y.S.2d 27, 2012 NY Slip Op 732 (App. Div. 2012); *Italfabrics, Ltd. v. Jay Jacobs, Inc.*, 1990 U.S. Dist. LEXIS 3643 (S.D.N.Y. April 5, 1990); *Kevin C. Stemp, A Comparative Analysis of the "Battle of the Forms"*, 15 *Transnat'l L. & Contemp. Probs.* 243 (2005). 9. *Boardman Steel Fabricators, Ltd. v. Andritz, Inc.*, 2015 U.S. Dist. LEXIS 119562, \*9-10 (E.D. Ky. Sept. 9, 2015). See *Kraft v. Health*, 2020 U.S. Dist. LEXIS 255115, \*19 (D. N.D. Dec. 3, 2020) (“To decide whether goods or services predominate in a mixed contract, courts often consider the contract language, the business of the supplier, and the ‘intrinsic worth’ of the goods involved. . . . Courts also commonly compare the relative cost between the goods and services in the contract.”) 10. See, e.g., *Am's Collectibles Network, Inc. v. Timily (HK)*, 746 F. Supp. 2d 914 (E.D. Tenn. 2010). 11. *Thyssenkrupp Metallurgical Prods. GmbH v. Energy Coal, S.p.A.*, 2015 NY Slip Op 31922(U) (Sup. Ct. 2015). 12. Ala. Code § 7-2-725(1). 13. Ala. Code § 6-2-34(9). 14. *Wadley Crushed Stone Co., LLC v. Positive Step, Inc.*, 2022 U.S. App. LEXIS 14014 (11th Cir. May 24, 2022).

15. E.g., *Hassler v. Circle C Res.*, 2022 WY 28, 505 P.3d 169 (2022). 16. Charles A. Sullivan, *The Puzzling Persistence of Unenforceable Contract Terms*, 70 *Ohio St. L.J.* 1127, 1159 (2009). 17. *Restatement of Employment Law* § 8.08, *Reporters Notes* (2015). *Heraeus Med., LLC v. Zimmer, Inc.*, 135 N.E.3d 150 (Ind. 2019) offered a spirited but unsatisfying defense of the strict blue-pencil approach. 18. *Restatement of Employment Law* § 8.08. 19. *Hassler*, 2022 WY 28 (excellent opinion).



Thione, regardless of what the parties’ intentions may have been . . . .”<sup>22</sup>

Drafters who seek to exclude consequential damages may not be excluding the damages they think they are. A federal court summed up the problem when it declared that a contractual provision excluding “consequential damages” is ambiguous. “The term ‘consequential damages’ is subject to multiple interpretations, and ‘no two courts or treatises define consequential damages the same way.’”<sup>23</sup> For drafters who rely on contract language excluding consequential damages, that judicial statement ought to be chilling. What’s the difference between direct and consequential damages? Both are foreseeable, but direct damages are more foreseeable than consequential damages.<sup>24</sup> But at what point on the foreseeability continuum does someone cross from one to the other? There are no bright lines.

For instance, while lost profits are usually regarded as consequential damages, sometimes they are direct damages.<sup>25</sup> The court in *Jay Jala, LLC v. DDG Constr., Inc.*<sup>26</sup> spent more than 3,000 words groping for clarity to decide whether various categories of damages fell within the consequential damages exclusion. The effort was valiant, but the court’s task was an impossible one. Parties can often avoid the squabbles over what is consequential damages by spelling out precisely how they want various categories of damages to be treated in the event of a breach, instead of simply excluding consequential damages. To simply exclude all consequential damages can be akin to inviting a stranger of indeterminate ability—otherwise known as a judge—to become an *ex post facto* co-drafter of the contract.

If a contract for the sale of goods has an effective sole and exclusive remedy (e.g., repair or replacement shall be the sole and exclusive remedy), and the seller is unable or unwilling to give the remedy stated, the remedy has failed of its essential purpose, and the buyer is entitled to the entire panoply of remedies available under the U.C.C.<sup>27</sup> But what happens if the contract also contains an exclusion of consequential damages? Most courts say that the exclusion is enforceable, but some courts say that the exclusion does not apply and that the buyer is entitled to consequential damages.<sup>28</sup> The parties must draft around it. Example: “Regardless of the failure of the sole and exclusive remedy, SUPPLIER will not be liable for any indirect, special, incidental, or consequential damages regardless of how they are characterized. The parties intend the exclusion of indirect, special, incidental, or consequential damages as

### Everybody Knows Basic Contract Law, Don’t They?

Few attorneys think that the law of offer and acceptance is in any sense controversial, though it can be. Consider these two cases:

■ **First.** Plaintiff sought to accept a settlement offer without a duration after the case proceeded to arbitration and an award was handed down that was less than the defendant’s settlement offer. The court held that the settlement offer had expired because a reasonable time had passed. A reasonable time is usually a fact issue, but a judge can decide the limits of a reasonable time where the facts are undisputed. “A reasonable time ‘is the time that a reasonable person in the exact position of the offeree would believe to be satisfactory to the offeror.’” The court noted that “Implicit in an offer (and an acceptance) to settle a personal injury suit is the party’s intent to avoid a less favorable result at the hands of a jury, a judge, or, in this case, an arbitrator.” The offer was designed to avoid the risk about the amount of the arbitration. But the circumstances here changed when the arbitrator set the value of the claim with the arbitration award—at that point, the offer had expired.<sup>20</sup>

■ **Second.** Wal-Mart, defendant in a slip-and-fall case, filed a motion for summary judgment. Subsequently, on March 29, 2017, Wal-Mart’s attorney made an offer via email to plaintiff’s counsel to settle the case by paying plaintiff, and it gave the plaintiff until 3:00 p.m. on Friday, March 31, 2017, to accept. The next morning, March 30, 2017, Wal-Mart’s summary judgment motion was granted. Less than one hour after receiving notice of the court’s disposition, the plaintiff’s counsel advised Wal-Mart’s counsel that plaintiff accepted Wal-Mart’s settlement offer. The court rejected Wal-Mart’s argument that the granting of summary judgment implicitly withdrew Wal-Mart’s settlement offer.<sup>21</sup>

The offers in the two cases differ because in the second case, the *Wal-Mart* offer stated a firm duration—until March 31 at 3 p.m.—so the offer did not expire in a reasonable time. Up to the time that the plaintiff accepted the settlement offer, Wal-Mart manifested no intention to revoke the offer based on a favorable disposition of its summary judgment motion, which certainly was foreseeable to Wal-Mart. Regardless, it was asking too much of the court to ignore the express terms of Wal-Mart’s settlement offer—its firm duration—under the facts of the case.

### Remedies

There are many traps for the unwary in drafting limitations of remedies. Merely stating a substitute remedy in the contract is not enough to make it exclusive—the contract has to say that it is the exclusive remedy. There is a presumption of cumulative remedies. Advanced BodyCare Solutions’ contract with Thione said that if Advanced “fail[ed] to order and pay for at least the minimum dollar amount of Products during any applicable period of time,” Thione could, “at [its] sole and absolute discretion,” terminate or renegotiate the Agreement, or revoke its exclusivity. Advanced claimed that these remedies were the only remedies available to Thione. The U.S. Court of Appeals for the Eleventh Circuit disagreed, noting courts’ “strong reluctance to construe a contractual remedy as exclusive” when the agreement did not use “the magic words ‘exclusive’ or ‘sole’ remedy”—and this is so “even when they have thought that an exclusive remedy was intended . . . .” The agreement “does not clearly express that the listed remedies are the exclusive remedies available to

<sup>20</sup> *Sherrod v. Kidd*, 138 Wn. App. 73, 155 P.3d 976 (2007). See also *Moore v. Donegal Mut. Ins. Co.*, 247 Md. App. 682, 693, 239 A.3d 764, 770 (2020) (“[W]here the offer was accepted prior to final judgment, within approximately two hours after the offer was stated to be still on the table, the issue whether the offer was accepted within a reasonable amount of time is an issue of fact.”) <sup>21</sup> *Wal-Mart Stores Tex. LLC v. Shirey*, 2020 Tex. App. LEXIS 945 (Feb. 4, 2020).

<sup>22</sup> *Advanced BodyCare Solutions, LLC v. Thione Int’l, Inc.*, 615 F.3d 1352, 1362 (11th Cir. 2010). See *Consolidation Coal Co. v. Marion Docks, Inc.*, 2010 U.S. Dist. LEXIS 32524, \*9 (W.D. Pa. Feb. 22, 2010), adopted, 2010 U.S. Dist. LEXIS 31365 (W.D. Pa. March 31, 2010). <sup>23</sup> *Team Contrs., LLC v. Waypoint NOLA, LLC*, 2017 U.S. Dist. LEXIS 160763, at \*10 (E.D. La. Sept. 29, 2017). See *DaimlerChrysler Motors Co., LLC v. Manuel*, 362 S.W.3d 160 (Tex. App. 2012) (distinction between direct and consequential damages remains elusive). <sup>24</sup> *Iron Branch Assocs., LP v. Hartford Fire Ins. Co.*, 2021 U.S. Dist. LEXIS 171601 (D. Del. Sept. 9, 2021). See Peter A. Alces, *On Discovering Doctrine: “Justice” in Contract Agreement*, 83 Wash. U. L. Q. 471, 484, n. 40 (2005). <sup>25</sup> *OMS3, LLC v. Carestream Dental, LLC*, 2020 U.S. Dist. LEXIS 202566 (E.D. Pa. Oct. 30, 2020). <sup>26</sup> *Jay Jala, LLC v. DDG Constr., Inc.*, 2016 U.S. Dist. LEXIS 150969 (E.D. Pa. Nov. 1, 2016). <sup>27</sup> U.C.C. § 2-719(2). <sup>28</sup> See, e.g., *Sanchelina Int’l, Inc. v. Walker Stainless Equip. Co., LLC*, 920 F.3d 1141 (7th Cir. 2019); *Eastern Fisheries, Inc. v. Aircas United States, LLC*, 2016 U.S. Dist. LEXIS 195021 (D. Mass. Jan. 28, 2016).



an independent agreement apart from the sole and exclusive remedy referenced herein.”

In recent years, parties on the losing end of breach of contract actions sometimes unexpectedly find themselves responsible for attorney’s fees. This is because in many courts, broadly drafted indemnity clauses are being applied to first-party claims. While indemnity traditionally has been deemed to apply to third-party claims, in recent years, more litigants have attempted to use indemnity provisions in connection with first-party claims (that is, direct breach of contract claims between the parties to the contract where no third-party is involved). This means that if the indemnity provision contains an attorney’s fee provision, the non-prevailing party must pay. For example, a broadly drafted indemnification clause covering “any and all costs and expenses” may be held to include first-party claims.<sup>29</sup> Many drafters are now policing indemnity provisions more closely to ensure that they are applied only to third-party claims.

### Parol Evidence

No area of contract law is more misunderstood than the parol evidence rule (except, of course, the battle of the forms,<sup>30</sup> which is in its own universe in terms of misapprehension). The parol evidence rule is very often mistaken as an aid to interpreting contracts. It is nothing of the kind. When judges say that “parol evidence is not admissible unless the contract

is ambiguous,” this is not a statement of the parol evidence rule, it is a statement of interpretation—in that instance, it is unfortunate that judges use the term parol evidence instead of extrinsic evidence.

The parol evidence rule deals with integration, not interpretation. The court must first decide the integration question—that is, the scope of the agreement (specifically, whether the parties intended for the writing to bar admission of evidence of prior or contemporaneous agreements).<sup>31</sup> Only after figuring out which terms are part of the agreement may the document be interpreted.<sup>32</sup> Ambiguity goes to interpretation, not integration.

A merger clause gives full effect to the parol evidence rule—it says that “there are no representations, promises or agreements between the parties except those found in the writing.”<sup>33</sup> Are merger clauses conclusive on the question of integration? Some courts say they are;<sup>34</sup> some say they are not, but that they are significant.<sup>35</sup> The most important rule about merger clauses is to have one. In one case, the U.S. Court of Appeals for the Second Circuit held that because there was no merger clause, it was proper for the lower court to admit evidence of a prior agreement as shown by a text message thread and a photo of a white board from a meeting<sup>36</sup>— exactly the sort of evidence that merger clauses are designed to exclude.

<sup>29</sup> E.g., *Hensel Phelps Constr. Co. v. Cooper Carry Inc.*, 861 F.3d 267 (D.C. Cir. 2017). <sup>30</sup> U.C.C. § 2-207. <sup>31</sup> *Wachovia Bank, N.A. v. Dresdner (In re Brookland Park Plaza, LLC)*, 2009 Bankr. LEXIS 3241, \*18 n. 5 (Bankr. E.D. Va. Oct. 13, 2009) (the parol evidence rule “is not a rule of interpretation, but rather it defines the subject matter of interpretation.”) <sup>32</sup> Restatement (Second) of Contracts § 213, cmt. a. <sup>33</sup> Restatement (Second) of Contracts § 216 cmt. e (1981). <sup>34</sup> 1-5 *Murray on Contracts* § 85 (a merger clause states “that the writing constitutes the sole and exclusive repository of the parties’ agreement and somewhat redundantly [adds that the parties] do not intend to be bound by any other agreement, understanding or negotiation of whatsoever kind or nature.”); *Shehadeh v. Horizon Pharma USA, Inc.*, 2021 U.S. Dist. LEXIS 174508, \*12 (S.D.N.Y. Sept. 14, 2021). <sup>35</sup> E.g., *Zwiker v. Lake Superior State Univ.*, 2022 Mich. App. LEXIS 859, \*30 (Feb. 10, 2022). <sup>36</sup> E.g., *Bonfire, LLC v. Zacharia*, 251 F. Supp. 3d 47 (D.D.C. 2017) (merger clause may be a significant but not conclusive factor). <sup>37</sup> *Dhalwal v. Hypr Corp.*, 2022 U.S. App. LEXIS 781 (2d Cir. Jan. 11, 2022).

### Related Content

For a comprehensive collection of resources to assist counsel in drafting contractual dispute provisions, see

 [DRAFTING CONTRACTUAL DISPUTE PROVISIONS RESOURCE KIT](#)

For practical guidance in drafting and interpreting standard contractual and boilerplate clauses, see

 [GENERAL COMMERCIAL CONTRACT CLAUSE RESOURCE KIT](#)

For a discussion of common risk allocation mechanisms used in commercial contracts, see

 [RISK ALLOCATION IN COMMERCIAL CONTRACTS](#)

For a checklist outlining what counsel should consider when drafting or reviewing a commercial contract, see

 [COMMERCIAL CONTRACT DRAFTING AND REVIEW CHECKLIST](#)

For sample boilerplate clauses for use in commercial contracts, see

 [BOILERPLATE CLAUSES \(SHORT FORM\)](#)

For assistance in drafting choice of forum clauses for use in commercial contracts, see

 [CHOICE OF FORM CLAUSES](#)

Modern contract litigation often includes extra-contractual claims along with claims for breach of contract. A garden-variety merger clause may not preclude evidence of fraud in the inducement to invalidate the contract.<sup>37</sup> But some courts have suggested a drafting solution that precludes fraud claims—by including non-reliance language in the merger clause. In *SodexoMAGIC, LLC v. Drexel Univ.*,<sup>38</sup> the court was called upon to decide whether the following generic integration clause precluded fraud claims: “This Agreement contains all agreements of the parties with respect to matters

covered herein, superseding any prior agreements, and may not be changed other than by an agreement in writing signed by the parties hereto.” The clause mentions prior agreements but not prior representations. The court found that the clause, as written, did not preclude a claim for fraudulent inducement. Something more than a garden-variety integration clause was needed—a fraud insulating clause that would make it legally impossible for a party to establish that it justifiably relied on a pre-contractual representation. The panel called this an “integration-plus contract.”

Some invisible terms—trade usage and course of dealing—become part of the contract even with a garden-variety merger clause. (Trade usage and course of dealing are terms of art with established meanings.)<sup>39</sup> Unless they are carefully negated in the contract, the parties’ written expression is to be read as if it contained this evidence.<sup>40</sup> This careful negation requires words in addition to the usual merger clause.<sup>41</sup> Another invisible term—course of performance—refers to the conduct of the parties in carrying out the terms of their writing.<sup>42</sup> Since such evidence occurs after the writing, it cannot be precluded by the parol evidence rule—regardless of whether the writing has a merger clause.<sup>43</sup>

Traps for the unwary are everywhere in contract law. A few more short examples:

- **No oral modification.** A lot of people think that no oral modification (NOM) clauses are part of merger clauses but, of course, they are not. Merger clauses deal with prior or contemporaneous agreements; NOM clauses deal with post-formation agreements. While there are some statutes (e.g., in New York and the U.C.C.) that give NOM clauses more teeth, “[c]ourts applying the common law generally have been hostile to no-oral-modification clauses.”<sup>44</sup> “[A]ny clause purporting to annul subsequent modification is invalid.”<sup>45</sup> One court succinctly put it this way: “[A] ‘no oral modification’ clause may be waived by the parties by entering into an otherwise enforceable oral agreement.”<sup>46</sup> A roundabout way to help to keep oral modifications from being enforced is to include a provision stating that certain specified agents shall have no power to vary the contract or to waive the performance of conditions. A party who wishes to rely upon a subsequent waiver by the specified agent must show that in some way the agent acquired such power after the contract was made.

<sup>37</sup> *Vigortone Ag Prods. v. AG Prods.*, 316 F.3d 641, 644 (7th Cir. 2002) (“the majority rule is that an integration clause does not bar a fraud claim.”). *But see e.g., Pass v. Palmiero Auto. of Butler, Inc.*, 229 A.3d 1, 7 (Pa. Super. 2020) (“When the parties intend for a writing to be their entire contract, parol evidence is inadmissible to demonstrate fraud in the inducement of the contract, i.e., ‘an opposing party made false representations that induced the complaining party to agree to the contract.’” *Toy v. Metro. Life Ins. Co.*, 593 Pa. 20, 928 A.2d 186, 205 (Pa. 2007)). <sup>38</sup> *SodexoMAGIC, LLC v. Drexel Univ.*, 24 F.4th 183 (3d Cir. 2022). <sup>39</sup> E.g., U.C.C. § 1-303; Restatement (Second) of Contracts §§ 222-223. <sup>40</sup> U.C.C. § 2-202, cmt. 2. <sup>41</sup> *Precision Fitness Equip., Inc. v. Nautilus, Inc.*, 2011 U.S. Dist. LEXIS 13576 (D. Colo. Feb. 2, 2011). <sup>42</sup> U.C.C. § 1-303(a); Restatement (Second) of Contracts § 202(4). <sup>43</sup> See U.C.C. § 2-202, cmt. 2 (does not include course of performance among the matters that can be carefully negated). *See also Keith A. Rowley, Contract Construction and Interpretation: From the “Four Corners” to Parol Evidence (and Everything in between)*, 69 *Miss. L.J.* 73, 331 (1999) (course of performance cannot be “carefully negated”). <sup>44</sup> Michael M. Greenfield, *Consumer Protection and the Uniform Commercial Code: The Role of Assent in Article 2 and Article 9*, 75 *Wash. U. L. Q.* 289 (1997). <sup>45</sup> *George S. Geis, Gift Promises and the Edge of Contract Law*, 2014 *U. Ill. L. Rev.* 663, 677, n. 70 (2014).



client's obligations (as well as your client's right to seek damages)—but add a catch-all: “not excluding any conduct or event constituting material breach of contract, whether similar or dissimilar to this list.”

- **Statute of limitations.** Parties generally can shorten statutes of limitations so long as the time period allows a party a reasonable opportunity to assert a claim, but parties generally cannot extend the statutes of limitations.<sup>53</sup> If a warranty extends to future performance, it does not technically alter the statute of limitations, but it has the effect of doing just that. For most warranties for the sale goods, the breach occurs at the time of tender of delivery of the goods—and that is when the statute of limitations begins to run. If, however, a warranty promises that the goods will perform a certain way in the future, the warranty has been extended to future performance, and the statute of limitations will not start to run until the breach is or should have been discovered—potentially many years after the statute would run for a garden-variety warranty.<sup>54</sup>

On and on it goes. No one is able to fully keep up with contract law—the cases come too fast, dozens every day. All due apologies to Professor Williston: Professor Corbin was right. There are no final principles. As attorneys, it is our job to be sentries—always watching the skies for change in the law. Failure to heed the signs of change can be disastrous for our clients. ■

*Timothy Murray, a partner in the Pittsburgh, PA law firm Murray, Hogue & Lannis, is the lead author of the Corbin family of contract law texts. He writes the biannual supplements to Corbin on Contracts, is author of Corbin on Contracts, volumes 1 and 15 and volume 8 (pending publication); Corbin on Pennsylvania Contracts; Corbin on Ohio Contracts; Corbin on Massachusetts Contracts; Corbin on New York Contracts (publication pending); Corbin on Contracts: Force Majeure and Impossibility of Performance Resulting from COVID-19 (2021), and is co-author of Corbin on Contracts Desk Edition (2021) and Corbin on Contract Drafting (pending publication).*



RESEARCH PATH: [Commercial Transactions > General Commercial and Contract Boilerplate > Articles](#)

- **Anti-assignment.** According to some courts, an anti-assignment clause merely creates a duty in the promisor not to assign while not depriving the promisor of the power to assign. This means that even if the contract has an anti-assignment clause, the party bound by the clause has the power to make an assignment, but the assignment would constitute a breach of an anti-assignment provision.<sup>47</sup> It typically would be difficult to prove damages in that instance. To deprive a would-be assignor of the power to assign, the general view is that the contractual provision needs to use words making clear that any such attempted assignment is null and void or invalid,<sup>48</sup> or words to that effect.

- **Breach of contract.** There are generally speaking two kinds of breaches, material breaches and immaterial breaches. The non-breaching party injured by either can sue in order to prove and recover damages, but only a material breach will discharge the non-breaching party of its obligations under the contract.<sup>49</sup> The problem is that it is often difficult to tell whether a breach is material or non-material without a court order. Many courts employ the five-prong test,<sup>50</sup> a factually intense test,<sup>51</sup> to determine materiality—but if the non-breaching party wrongly treats an immaterial breach as a material breach and stops performing, the non-breaching party might be committing a material breach of its own.<sup>52</sup> To remove some of these issues from the trier of fact, draft the contract to specifically mention the conduct or events that will result in discharge of your

<sup>46.</sup> *Staff4jobs v. List Logistics*, 2022 U.S. Dist. LEXIS 33328, \*19 (D. N.J. Feb. 25, 2022). See *G.L.M. Sec. & Sound, Inc. v. LoJack Corp.*, 667 Fed. Appx. 339 (2d Cir. 2016) (despite an NOM clause, a modification may be implied by the parties' conduct) (Massachusetts law). <sup>47.</sup> *Restatement (Second) of Contracts* § 322(2)(b); *Brdl v. Rd Legal Funding*, 2021 N.J. Super. Unpub. LEXIS 643 (April 16, 2021) (Delaware law). But see *Travertine Corp. v. Lexington-Silverwood*, 683 N.W.2d 267, 272, 274 (Minn. 2004), which construes anti-assignment clauses as depriving the putative assignor of the power to assign. <sup>48.</sup> *Pravin Banker Assocs., Ltd. v. Banco Popular Del Peru*, 109 F.3d 850, 856 (2d Cir. 1997); *Brdl*, 2021 N.J. Super. Unpub. LEXIS 643. <sup>49.</sup> *Furnituredealer.Net, Inc. v. Amazon.com, Inc.*, 2022 U.S. Dist. LEXIS 54509, \*93-94 (D. Minn. March 25, 2022) (citing *Corbin on Contracts*). <sup>50.</sup> *Restatement (Second) of Contracts* § 241. <sup>51.</sup> *Bear, Stearns Funding, Inc. v. Interface Group -- Nev., Inc.*, 361 F. Supp. 2d 283, 296 (S.D.N.Y. 2005) (citing *Jacob & Youngs, Inc. v. Kent*, 230 N.Y. 239, 243, 129 N.E. 889, 891 (1921) (Cardozo, J)). <sup>52.</sup> *Kodak Graphic*, 2015 U.S. Dist. LEXIS 834, aff'd, *Kodak Graphic*, 640 Fed. Appx. 36. <sup>53.</sup> E.g., *John J. Kassner & Co. v. New York*, 46 N.Y.2d 544, 389 N.E.2d 99, 415 N.Y.S.2d 785 (1979). <sup>54.</sup> *Hoctor v. Polchinski Memos, Inc.*, 50 Misc. 3d 65 (N.Y. App. Term 2015).



Kenneth D. Kleinman and Brad M. Kushner STEVENS & LEE

## Whistleblower Complaint Response and Defense Strategies under Section 11(c) of the Occupational Safety and Health Act

This article addresses strategies for responding to and defending against whistleblower complaints filed under Section 11(c) of the Occupational Safety and Health Act (the OSH Act).<sup>1</sup> The OSH Act regulates employment conditions relating to occupational safety and health. Every person engaged in a business affecting commerce is required to furnish each employee employment and a place of employment free from recognized hazards that are causing or are likely to cause death or serious physical harm and to comply with occupational safety and health standards promulgated under the OSH Act.

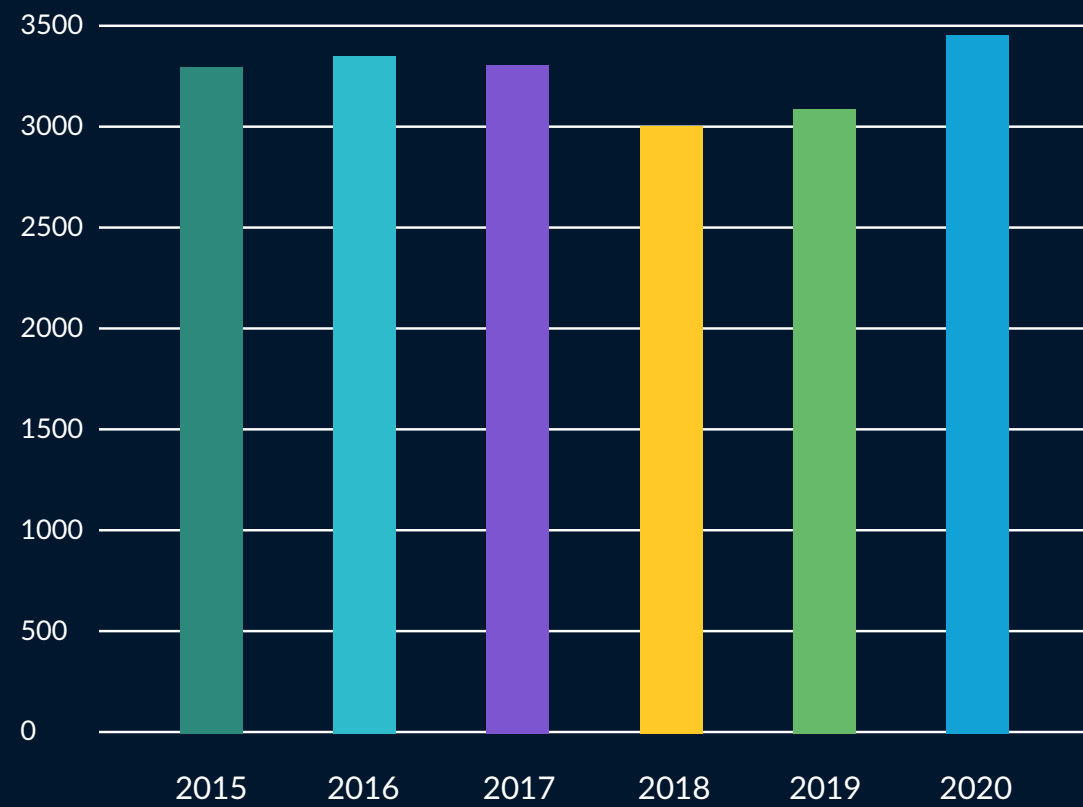


AS DETAILED BELOW, ONE OF THE KEY FEDERAL AGENCIES that handles whistleblower complaints is the Occupational Safety and Health Administration (OSHA). Below is a chart

showing data from OSHA on the number of whistleblower complaints filed with OSHA from 2015–2020. OSH Act whistleblower complaints increased during COVID-19.

<sup>1.</sup> 29 U.S.C.S. § 660(c).

## Whistleblower Complaints Received by OSHA (2015-2020)

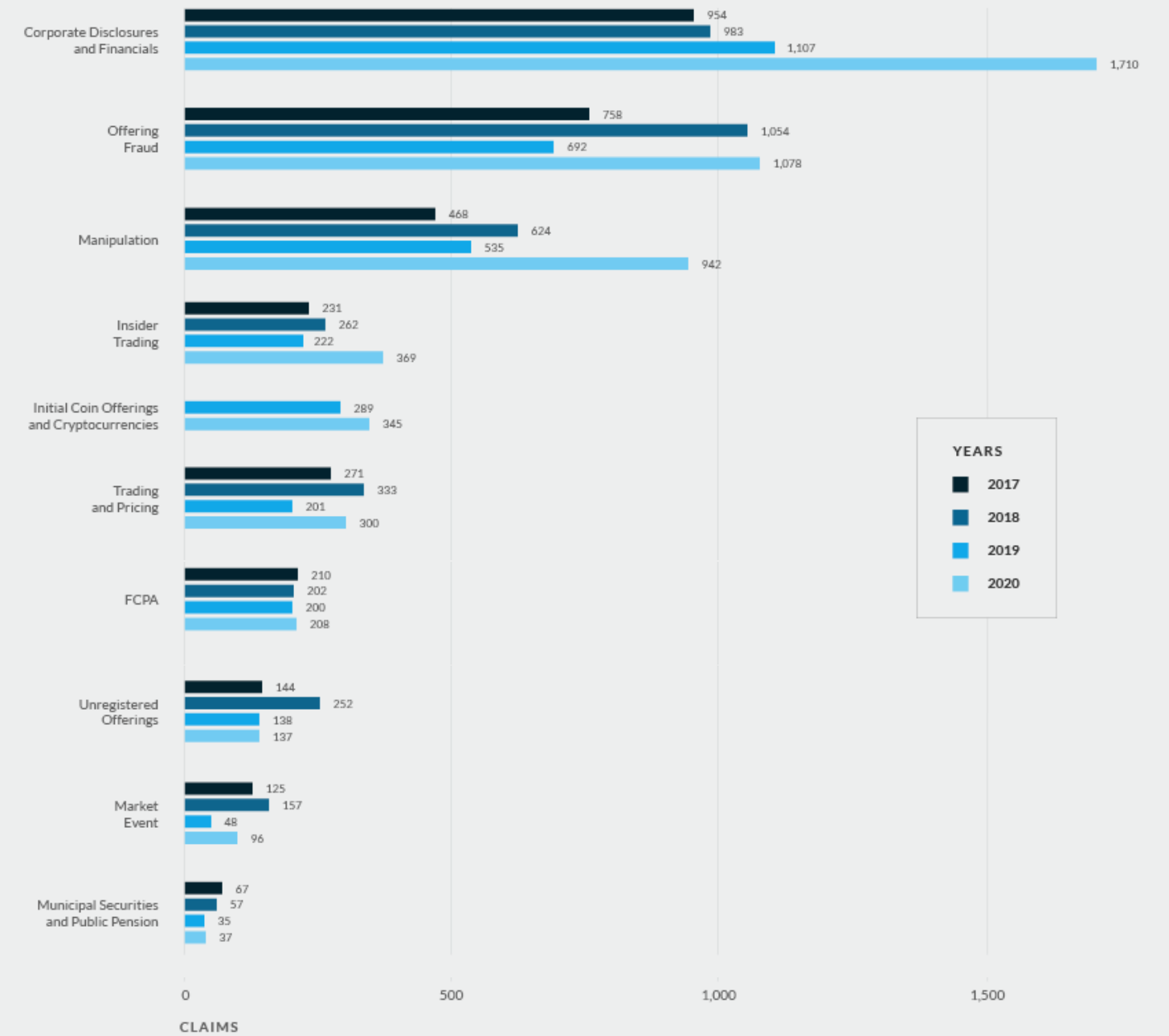


Visualization of Whistleblower Complaints Received by OSHA (2015-2020).

Source: [OSHA](#)

As detailed below, the Securities and Exchange Commission (SEC) also receives many whistleblower complaints. Below is a chart with data from the SEC showing the types and numbers of whistleblower claims that the SEC received from 2017-2020.

## SEC Whistleblower Tips Received by Claim Type (2017-2020)

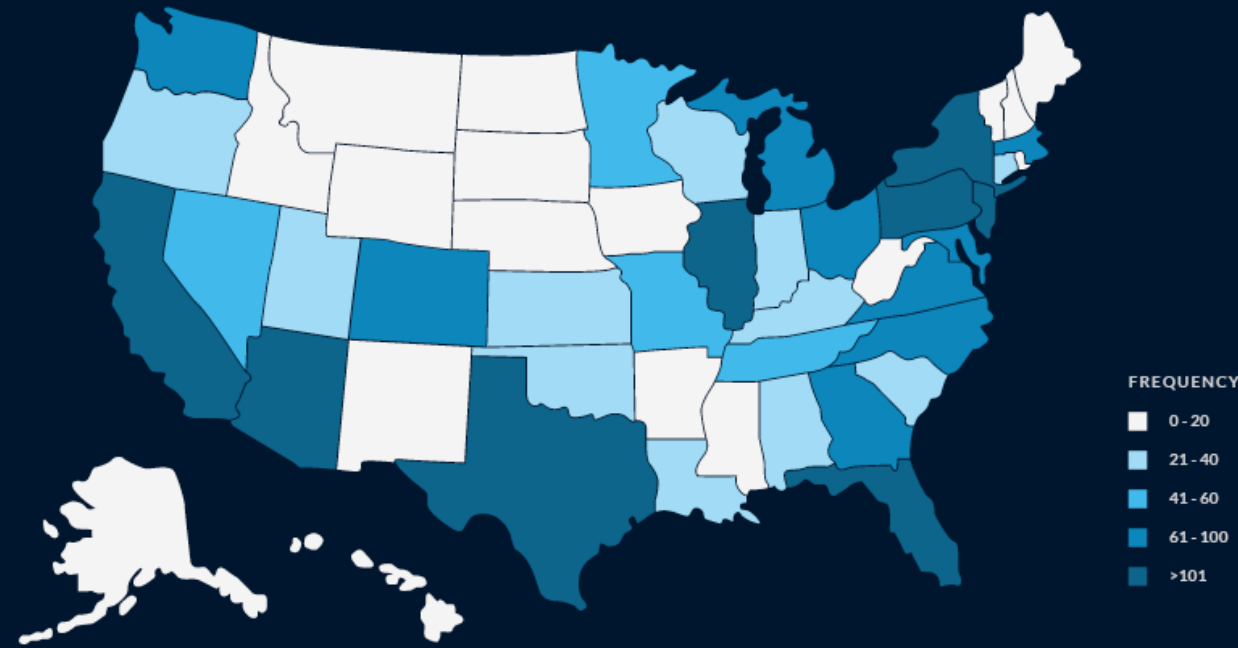


Visualization of SEC Whistleblower Tips Received by Claim Type (2017-2020).

Source: [SEC data](#).

Below is a chart with data from the SEC showing state-by-state whistleblower claims that the SEC received in 2020.

### SEC Whistleblower Tips Received by State (2020)



Visualization of SEC Whistleblower Tips Received by Claim Type (2017-2020).

Source: SEC data.

#### Elements of an OSH Act Whistleblower Action

Separate from the substantive safety and health standards, Section 11(c) of the OSH Act provides that no person shall discharge or in any manner discriminate against any employee because the employee has:

- Filed any complaint under or related to the OSH Act
- Instituted or caused to be instituted any proceeding under or related to the OSH Act
- Testified or is about to testify in any proceeding under the OSH Act or related to the OSH Act
- Exercised on his or her own behalf or on behalf of others any right afforded by the OSH Act<sup>2</sup>

#### Coverage of OSH Act Whistleblower Provisions

Any employee of a private-sector employer engaged in a business affecting interstate commerce is protected by Section 11(c). Employees of the U.S. Postal Service (USPS) are also covered by the OSH Act. Other than USPS employees, public-sector employees are not covered by Section 11(c).

#### Persons Prohibited from Discriminating and Retaliating

Section 11(c) states that “no person shall discharge or in any manner discriminate against any employee” because the employee has exercised rights under the OSH Act. The OSH Act defines person as “one or more individuals, partnerships, associations, corporations, business trusts, legal representatives, or any group of persons.” Thus, the

prohibitions of Section 11(c) are not limited to actions taken by employers against their own employees. Section 11(c) also extends to unions, employment agencies, or any other person in a position to discriminate against an employee.<sup>3</sup>

#### Persons Protected from Discrimination and Retaliation

Section 11(c) protects employees, which are defined as “an employee of an employer who is employed in a business of his employer which affects commerce.”<sup>4</sup> The OSH Act does not define the term employ. Courts determine the existence of an employment relationship, for purposes of Section 11(c), based upon economic realities.<sup>5</sup> (“[T]he broad remedial nature of this legislation demonstrates a clear congressional intent that the existence of an employment relationship, for purposes of Section 11(c), is to be based upon economic realities rather than upon common law doctrines and concepts.”) (citations omitted).

For purposes of Section 11(c), even an applicant for employment may be considered an employee.<sup>6</sup>

#### Occupational Safety and Health Administration (OSHA) Whistleblower Complaint Process for OSH Act Claims

A complaint under Section 11(c) typically begins when an employee or employee representative files a complaint with OSHA. After an investigation, OSHA determines whether to file an action in federal court on behalf of the aggrieved employee. This process is described below.

#### Filing the Complaint

Any applicant for employment, employee, former employee, or their authorized representative is permitted to file a whistleblower complaint with OSHA. No particular form of complaint is required. The complaint may be in any language and need not be in writing. OSHA also accepts electronically filed complaints on its Whistleblower Protection Program website.<sup>7</sup>

A complaint must include, at a minimum:

- The complainant’s full name, address, and phone number
- The name, address, and phone number of the respondent or respondents
- The date of filing
- The date of adverse action
- A brief summary of the alleged retaliation addressing the prima facie elements of a violation<sup>8</sup>

#### Investigating the Complaint

After a complaint is filed, an investigator is assigned to conduct complaint intake and determine whether the complaint alleges facts sufficient to make a prima facie showing of retaliation. Many complaints are dismissed at this stage.

If the investigator determines that an investigation is warranted, the investigator will:

- Interview the complainant and any witnesses
- Obtain statements and documentary evidence
- Interview and obtain statements from respondents’ officials
- Review pertinent records
- Take any other actions necessary to gather evidence and assess the complainant’s claims and the respondent’s defenses

As the respondent’s legal counsel, you have the right to be present for any management interviews. Ultimately, the investigator will make a recommendation regarding whether the complaint appears to have merit.<sup>9</sup>

During an investigation, OSHA must disclose to the respondent (or the respondent’s legal counsel):

- The filing of the complaint
- The allegations contained in the complaint
- The substance of the evidence supporting the complaint<sup>10</sup>

OSHA will provide to the complainant (or the complainant’s legal counsel) the substance of the respondent’s response. OSHA will redact any information that may compromise the identity of potential confidential witnesses and other confidential or sensitive information.<sup>11</sup>

#### Issuing a Determination

OSHA previously instructed investigators that a violation may be found if it was supported by a preponderance of the evidence. It lowered this burden in 2015, and OSHA now takes the position that investigators should determine whether there is reasonable cause to believe that Section 11(c) was violated.<sup>12</sup>

According to OSHA, this means that an investigator should determine whether a reasonable judge could find that a violation occurred, and “[t]he evidence does not need to establish conclusively that a violation did occur.”<sup>13</sup>

Section 11(c)(3) provides that the Secretary of Labor (Secretary) must notify a complainant of the Secretary’s determination

2. *Id.*

3. 29 C.F.R. § 1977.4. 4. 29 C.F.R. § 1977.5(a). 5. *Id.* 6. 29 C.F.R. § 1977.5(b). 7. U.S. Dept. of Labor, The Whistleblower Protection Program. 8. See Whistleblower Investigations Manual: Directive Number CPL 02-03-007 (Whistleblower Manual) at 2-2. 9. See Whistleblower Manual at 1-4. 10. See Whistleblower Manual at 23-6. 11. *Id.* 12. See Whistleblower Manual at 3-5, 3-6. 13. See “Clarification of the Investigative Standard for OSHA Whistleblower Investigations,” memorandum from Directorate of Whistleblower Protection Programs. See Whistleblower Manual at 3-6.



within 90 days of the filing of the complaint. However, this 90-day provision is considered directory, rather than mandatory, and the Secretary's failure to meet this timeline does not bar further investigation and does not affect the Secretary's ability to file in federal court.<sup>14</sup>

### Encouraging Settlement

It is OSHA's policy to seek settlement of all cases determined to be meritorious prior to referring the case for litigation. Further, at any point prior to the completion of an investigation, OSHA will attempt to resolve complaints in which both parties seek a resolution, either informally or through its early resolution program.<sup>15</sup>

### OSHA's Early Resolution Program

OSHA has implemented an early resolution program that enables the parties to a whistleblower complaint to attempt to resolve a complaint before a full investigation occurs. The early resolution process can be launched either before the case is assigned for an investigation, or at any point while an investigation is ongoing. The investigation is stayed while the parties attempt to resolve the case with the assistance of a neutral OSHA representative. Information obtained by the neutral representative during the early resolution process is confidential and is not disclosed to OSHA's investigative staff. Should the parties fail to reach a settlement, the case will be transferred to an investigator to start or resume investigation of the complaint.

While parties may request that the case be submitted to the early resolution program at any point during the investigation process, as a general rule, parties may only submit their case to the program one time.<sup>16</sup>

### OSHA's Requirements for Settlement Agreements

OSHA generally requires that any settlement agreement to which it is a party contain the elements outlined below, though these may be tailored to fit the particular situation:

- It must be in writing.
- It must stipulate that the respondent agrees to comply with the relevant statute(s).
- It must specify the relief obtained.
- It must address a constructive effort to alleviate any chilling effect, where applicable, such as a posting (including electronic posting, where the respondent communicates with its employees electronically) or an equivalent notice. If a posting or notice is not included in the settlement agreement the case file should contain an explanation.<sup>17</sup>

Employers and employees may resolve disputes between themselves and enter into private settlement agreements to which OSHA is not a party. To end OSHA's investigation or lawsuit, a private agreement must be approved by OSHA.

OSHA will approve a private settlement if it deems it to be:

- Fair
- Adequate
- Reasonable
- Consistent with the purpose and intent of Section 11(c)
- In the public interest

OSHA will not approve a whistleblower settlement agreement that contains provisions that may discourage whistleblowing, such as:

- Provisions that require employees to waive the right to receive a monetary award from a government-administered whistleblower award for providing information to a government agency about violations of the law
- Provisions that require an employee to advise the employer before voluntarily communicating with the government or to affirm that the employee is not a whistleblower<sup>18</sup>

If the parties do not submit their agreement to OSHA or if OSHA does not approve the signed agreement, OSHA may dismiss the complaint or continue its investigation.

Employers and their counsel should be aware that OSHA often issues press releases announcing the terms of settlements, including the monetary components.

### Pursuing a Section 11(c) Claim in Federal Court

If OSHA finds merit and the case cannot be settled, the Secretary will file a civil action in federal court against the person who committed the violation.<sup>19</sup> There is no private right of action under Section 11(c).<sup>20</sup> The Secretary in a federal court action is represented by the Regional Solicitor's Office.

There is no statute of limitations for the Secretary to file an action in federal court after notifying the parties of the outcome of an investigation. However, courts have held that the doctrine of laches may apply if the Secretary's delay was unreasonable and inexcusable and the delay has resulted in prejudice to the defendant.<sup>21</sup>

### Some States Recognize a Private Right of Action

Note, however, that some states do recognize a private right of action under state law for wrongful discharge based on public policy where an employee is discharged in retaliation for raising a safety complaint.<sup>22</sup> Other states hold that any such complaint is preempted by Section 11(c).<sup>23</sup>

### Remedies Available for a Section 11(c) Complainant

Section 11(c) provides: "In any such action the United States district courts shall have jurisdiction, for cause shown to restrain violations of paragraph (1) of this subsection and order all appropriate relief including rehiring or reinstatement of the employee to his former position with back pay."

Courts have interpreted this provision broadly to include:

- Lost wages
- Medical expenses
- Travel and housing expenses
- Emotional distress damages
- Prejudgment interest<sup>24</sup>

### Reinstatement

Reinstatement of the complainant to his or her former position is the presumptive remedy in whistleblower cases involving a discharge or demotion. Where reinstatement is not feasible, front pay in lieu of reinstatement may be awarded from the date of the award up to a reasonable amount of time for the complainant to obtain another job. Situations where front pay may be appropriate include:

- Those in which the respondent's retaliatory conduct has caused the complainant to be medically unable to return to work
- Where the complainant's former position or a comparable position no longer exists
- Where reinstatement might lead to extreme hostility or debilitating anxiety or other risks to the complainant's mental health

If a complainant seeks front pay, consider retaining an economic and/or a vocational expert to limit a potential front pay award.

### Back Pay

Back pay is typically calculated by deducting the complainant's interim earnings (from sources such as interim employment and workers' compensation payments) from the complainant's total earnings (before taxes and other deductions) that the complainant would have earned during the period of unemployment. It typically includes any cost-of-living increases or raises that the complainant would have received if he or she had continued to work for the respondent, if supported by competent evidence. A back pay award may also include compensation for lost bonuses, overtime, benefits, raises, and promotions.

Complainants have a duty to mitigate their damages. To be entitled to back pay, a complainant must exercise reasonable diligence in seeking alternate employment. Employers may wish to consider whether it is appropriate and feasible to make an offer of reinstatement to a complainant to limit back pay exposure. A respondent's cumulative liability for back pay ceases when a complainant rejects a bona fide offer of reinstatement to a job substantially equivalent to the complainant's former position.

14. See *Marshall v. N. L. Industries, Inc.*, 618 F.2d 1220, 1224 (7th Cir. 1980) (Secretary's failure to comply with 90-day provision did not bar action in federal court against employer); *Donovan v. Freeway Const. Co.*, 551 F. Supp. 869, 878 (D.R.I. 1982) (Secretary's failure to notify discharged employees within 90 days of complaint of Secretary's determination to proceed against employer did not prohibit institution and prosecution of action against employer). 15. See *Whistleblower Manual* at 6-12, 6-13. 16. See OSHA DIRECTIVE NUMBER: CPL 02-03-006 (Alternative Dispute Resolution (ADR) Processes for Whistleblower Protection Program). 17. See *Whistleblower Manual* at 6-15. 18. See *Whistleblower Manual* at 6-19, 6-20.

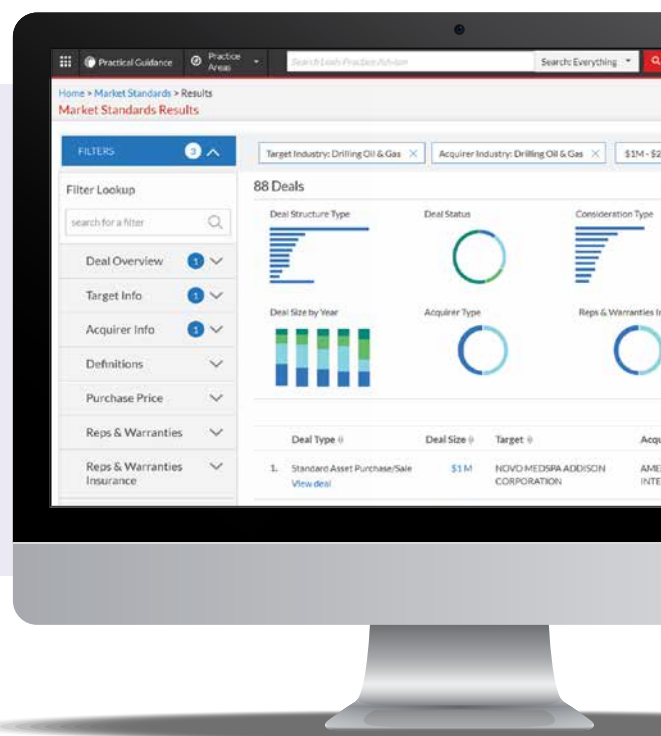
19. 29 U.S.C.S. § 660(c)(2). 20. *Donovan v. Occupational Safety & Health Rev. Comm.*, 713 F.2d 918, 926 (2d Cir. 1983); *George v. Aztec Rental Ctr. Inc.*, 763 F.2d 184, 186 (5th Cir. 1985); *Taylor v. Brighton Corp.*, 616 F.2d 256, 258-64 (6th Cir. 1980). 21. *Donovan v. Square D Co.*, 709 F.2d 335, 340 (5th Cir. 1983); *Marshall v. Intermountain Elec. Co.*, 614 F.2d 260, 263 (10th Cir. 1980). 22. See *Pytlinski v. Brocar Prods., Inc.*, 760 N.E.2d 385 (Ohio 2002) (terminated employee who alleged he had delivered a memorandum to his employer detailing violations of OSHA regulations in the workplace stated a valid claim); *Cloutier v. Great Atl. & Pac. Tea Co., Inc.*, 436 A.2d 1140 (N.H. 1981) (permitting recovery for wrongful discharge in violation of a public policy tenuously premised on duties imposed under OSHA). 23. See *McLaughlin v. Gastrointestinal Specialists, Inc.*, 750 A.2d 283 (Pa. 2000) (holding that OSHA provides the exclusive remedy for employees that claim retaliatory termination based on an OSHA complaint); *Walsh v. Consolidated Freightways*, 563 P.2d 1205 (Ore. 1977) (holding that plaintiff's claim of wrongful termination for raising workplace safety concerns was preempted by OSHA). 24. See *Reich v. Cambridgeport Air Sys., Inc.*, 26 F.3d 1187, 1194 (1st Cir. 1994) ("We conclude . . . that the statutory power to award "all appropriate relief" gave the district court authority, where such relief is in fact appropriate, to award compensatory and even such traditional other relief as exemplary damages."); *Martin v. H.M.S. Direct Mail Service, Inc.*, 936 F.2d 108, 109 (2d Cir. 1991) (holding that prejudgment interest is an appropriate component of a back pay award in a Section 11(c) case).



# MARKET STANDARDS

Search, Compare, Analyze  
More Public M&A Deals

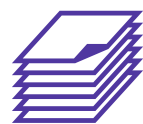
**Data-Driven Practical Guidance for M&A Attorneys**  
Market Standards helps M&A attorneys search and compare transactions using highly negotiated deal points, easily find precedent language, and see deal point and transactional trends with data visualizations.



**COMPARED TO OTHER OFFERINGS\***



33,000 deals  
(6x more)



150 deal points  
(2x more detail)



Sec updates within  
48 hours (3x faster)

See how Market Standards can boost your efficiency  
and give you an edge in your M&A deals.

LexisNexis.com/LexisPracticalGuidance | Call us today at 800.628.3612.

**Compensatory Damages**

A successful Section 11(c) complainant may also be entitled to an award of compensatory damages, which typically includes both pecuniary losses resulting from the adverse action, as well as damages to compensate the complainant for emotional distress, pain and suffering, loss of reputation, personal humiliation, and mental anguish suffered as a result of the adverse action.

Compensable pecuniary losses may include, for example, out-of-pocket medical expenses resulting from the cancellation of a company health insurance policy and medical expenses for treatment of symptoms directly related to the retaliation (e.g., post-traumatic stress, depression, etc.). They may also include:

- Vested fund or profit-sharing losses
- Credit card interest and other property loss resulting from missed payments
- Annuity losses

Successful complainants may also recover expenses incurred as a result of searching for other employment.

A successful complainant in a Section 11(c) action may also be awarded compensatory damages for emotional distress, pain and suffering, loss of reputation, personal humiliation, and mental anguish resulting from the respondent's adverse employment action. Emotional distress is not presumed.

Generally, a complainant must provide evidence of both:

- Objective manifestations of distress
- A causal connection between the retaliation and the distress

Objective manifestations of emotional distress include, but are not limited to:

- Depression
- Post-traumatic stress disorder
- Anxiety disorders

Objective manifestations also may include conditions that are not classified as mental disorders such as sleeplessness, harm to relationships, and reduced self-esteem.

Because a complainant must prove a causal connection between the retaliation and the emotional distress for which the complainant seeks compensation, you should explore in discovery whether there may be other causes for a complainant's emotional distress.

Courts generally do not require medical evidence to support a claim of emotional distress under Section 11(c).<sup>25</sup> However, evidence from a healthcare provider is required if a complainant seeks to prove a specific and diagnosable medical condition.

**Punitive Damages**

Courts may award a complainant in a Section 11(c) action punitive damages to punish the employer for violations in which respondents are aware that they are violating the law or where the violations involved egregious misconduct. There is no statutory cap on punitive damages under Section 11(c).

A respondent's good faith is a defense to punitive damages. Thus, a respondent may successfully defend against punitive damages if it can demonstrate that, for instance, its managers were acting on their own and contrary to a clear, consistently enforced anti-retaliation policy. To establish this defense, an employer will likely need to show not only that such a policy exists, but also that the offending manager was disciplined or terminated for violating it.

**Nonmonetary Remedies**

Remedies may also include:

- Non-monetary components (e.g., injunctive relief, expungement of warnings, reprimands, and derogatory references in a complainant's personnel file)
- Providing the complainant with a neutral reference for future employers
- Non-retaliation training for managers and/or employees
- The posting of notices regarding employees' Section 11(c) rights

**Best Practices and Strategies for Defending OSH Act Whistleblowing Complaints**

This section provides tips and strategies for defending a Section 11(c) complaint at the investigative stage and in a subsequent federal court action.

**Draft an Effective Position Statement**

A position statement submitted to OSHA is an employer's first opportunity to offer context and provide perspective on the facts and circumstances surrounding a Section 11(c) claim. A well-written, persuasive position statement can mean the difference between dismissal of a complaint at the administrative stage or years of costly litigation. At the same time, you should use caution when drafting position statements because any admissions or inconsistencies may

<sup>25</sup> See *Acosta v. Fairmount Foundry, Inc.*, 2019 U.S. Dist. LEXIS 232592, at \*1, n.1 (E.D. Pa. Feb. 6, 2019) (holding that plaintiff's testimony regarding his emotional distress was sufficient to overcome a summary judgment motion).

be used against the respondent during the investigation or in subsequent litigation. Keep in mind that the contents of a position statement and any supporting documents may be subject to public disclosure through a Freedom of Information Act request, so confidential information should be redacted or filed separately.

#### Use Easy-to-Follow Narratives

Most OSHA investigators are not attorneys. Thus, effective position statements should consist of an easy-to-follow narrative. Legal citations should be used sparingly and only if they are critical to the respondent's arguments. It may be useful to divide the position statement into two sections: one setting forth the facts and background, and the other explaining precisely why the complaint should be dismissed.

#### Attach Supporting Documentation

It is often helpful to attach supporting documentation that illustrates or corroborates the respondent's defenses. For example, witness statements, personnel and training records, company policies, and other documents that support the respondent's position may be included as exhibits. While not critical, you should consider attaching examples of company safety policies to demonstrate to OSHA the respondent's overall commitment to safety.

#### Consider Providing Evidence to Rebut Allegations

You should also be aware that a retaliation investigation may lead to a separate investigation of a violation of a substantive safety or health standard. By way of example, if an employee complains that he or she was discharged for reporting a lack of personal protective equipment (PPE), OSHA may investigate not only the complainant's retaliation claim, but also whether the employer violated a standard requiring it to provide employees with PPE. Thus, if a Section 11(c) complaint is based on a complainant's allegation of a substantive safety or health violation, you should consider providing evidence to rebut that allegation as well as the retaliation claim.

#### Consider Seeking Dismissal Based on a Failure to Meet Statutory Requirements

Below are some threshold considerations for respondents to consider when defending against a Section 11(c) complaint.

#### Is the Complainant an Employee?

Assess whether the complainant falls within the statutory definition of an employee protected by Section 11(c).<sup>26</sup>

#### Was the Complaint Timely?

Section 11(c) requires that complaints be filed with OSHA within 30 days of an alleged adverse action. Because of this short time frame, many Section 11(c) complaints are screened out or dismissed because the complainant has failed to timely file the complaint. Either after a complaint is filed with OSHA or after the Secretary files an action in federal district court, consider whether a complainant has met this deadline.

The first day of the 30-day period is the day after the alleged retaliatory decision is both made and communicated to the complainant. Generally, the date of the postmark, facsimile

#### Related Content

For more guidance on key Occupational Safety and Health Act (OSH Act) legal issues, see

 [OSH ACT REQUIREMENTS, INSPECTIONS, CITATIONS, AND DEFENSES](#)

For a discussion on the impact of the OSH Act on an employer's maintenance of a safe workplace in view of the COVID-19 pandemic, see

 [COVID-19 AND OSHA](#)

For tracking of recent agency rules regarding employer requirements and penalties under the OSH Act and other key federal, state, and local labor and employment legal developments, see

 [LABOR & EMPLOYMENT KEY LEGAL DEVELOPMENTS TRACKER \(CURRENT\)](#)

For a comprehensive survey of state occupational safety and health plan laws, including health and safety laws and posting requirements that are not part of Occupational Safety and Health Administration approved state plans, see

 [OCCUPATIONAL SAFETY AND HEALTH PLAN STATE LAW SURVEY](#)

For a listing of each state's practice notes on state OSH Act compliance, employee health, and workplace security issues in Practical Guidance's Labor & Employment offering, see

 [OSH ACT COMPLIANCE, EMPLOYEE HEALTH, AND WORKPLACE SECURITY STATE PRACTICE NOTES CHART](#)



transmittal, email communication, telephone call, hand-delivery, delivery to a third-party commercial carrier, or in-person filing at a Department of Labor office is considered the date of filing. If the postmark is absent or illegible, the date filed is the date the complaint is received. If the last day of the statutory filing period falls on a weekend or a federal holiday, or if the relevant OSHA office is closed, the next business day will count as the final day.

Because Section 11(c) does not require any particular form of complaint, a complaint need not be reduced to writing to meet the 30-day deadline.<sup>27</sup>

Additionally, because many complaints under Section 11(c) also raise claims under Sections 7 and 8 of the National Labor Relations Act, which has a six-month charge-filing period, OSHA often refers untimely Section 11(c) complaints to the National Labor Relations Board for investigation under that statute.

Note also that the 30-day statute of limitations may be equitably tolled:

[T]here may be circumstances which would justify tolling of the 30-day period on recognized equitable principles or because of strongly extenuating circumstances, e.g., where the employer has concealed, or misled the employee regarding the grounds for discharge or other adverse action; or where the discrimination is in the nature of a continuing violation. The pendency of grievance-arbitration proceedings or filing with another agency, among others, are circumstances which do not justify tolling the 30-day period. In the absence of circumstances justifying a tolling of the 30-day period, untimely complaints will not be processed.<sup>28</sup>

#### Consider Whether the Secretary Has Established a Prima Facie Case

OSHA and courts considering retaliation claims under Section 11(c) apply the burden-shifting framework established in *McDonnell Douglas Corp. v. Green*.<sup>29</sup>

<sup>26</sup> While the statute's reach is broad, there may be instances when the complainant's relationship to the respondent is too attenuated to create an employment relationship under Section 11(c) and 29 C.F.R. § 1977.5.

<sup>27</sup> See *Acosta v. Dura-Fibre LLC*, 2018 U.S. Dist. LEXIS 89536, at \*19 (E.D. Wis. May 30, 2018) (holding that a complainant's telephone call to OSHA area office was sufficient to satisfy the statute of limitations). <sup>28</sup> 29 C.F.R. § 1977.15(d)(3). See also *Donovan v. Hahner, Foreman & Harness, Inc.*, 736 F.2d 1421, 1428 (10th Cir. 1984) (finding that equitable tolling of 30-day period was appropriate where employer misled employee into believing that he had been laid off rather than fired and employee made diligent efforts to discover his true employment status). <sup>29</sup> 411 U.S. 792, 93 S. Ct. 1817, 36 L. Ed. 2d 668 (1973).



In considering causation, OSHA and the courts analyze whether protected activity was a but for cause for the adverse action.

Adverse actions that may support a retaliation claim are not “limited to discriminatory actions that affect the terms and conditions of employment” and may also include, for example, a lateral transfer, an unfavorable job reference, or a change in work schedule.<sup>35</sup> While some actions, such as terminations and demotions, clearly qualify as adverse actions, others are context-specific.<sup>36</sup>

Thus, where a complainant was not discharged or demoted, you should consider whether a fact finder would deem the action sufficiently adverse such that a reasonable worker would be dissuaded from engaging in activity protected by Section 11(c).

*Is There a Causal Link between Protected Activity and the Adverse Action?*

Another way to defeat a Section 11(c) claim is to demonstrate a lack of causation. A complainant in a Section 11(c) case must establish a causal link between his or her protected activity and the subsequent adverse employment action. While it is the Secretary’s burden to establish causation, you should consider whether you can present evidence to rebut the existence of a causal link.

In considering causation, OSHA and the courts analyze whether protected activity was a but for cause for the adverse action.<sup>37</sup>

Evidence of causation may be direct or circumstantial and may include:

- Suspicious timing
- Ambiguous statements or behavior toward the employee who engaged in protected activity
- Evidence that similarly situated employees who did not engage in protected activity received better treatment
- Evidence that the employer offered a pretextual reason for an adverse employment action

In the absence of direct evidence of causation, the Secretary may rely upon close temporal proximity to infer a causal link. However, courts are divided on whether close temporal proximity alone may establish causation.<sup>38</sup>

Often, protected activity is not in dispute, such as in situations where an employee complained to OSHA about an unsafe condition or participated in an OSHA investigation. Additionally, OSHA and courts take a broad view regarding what other types of activities are protected.<sup>32</sup>

Still, there are instances when a respondent may be able to show that a complainant did not engage in activity protected under Section 11(c). A complainant may erroneously characterize an ordinary workplace complaint as one involving safety or health. For example, an employee might object to performing a particular assignment based on his or her preference but later claim that the objection was based on a safety or health concern. In such a situation, the employer should present evidence or testimony establishing that the employee’s objection was not based on a safety or health concern, and thus was not protected under Section 11(c).

A complaint also is not protected activity if it is not made in good faith.<sup>33</sup> Thus, consider whether a complainant had an ulterior motive in lodging a complaint.

*Did the Complainant Suffer an Adverse Action?*

Another way to defeat a Section 11(c) claim is to rebut a complainant’s assertion of an adverse action. To prevail on a retaliation claim under Section 11(c), a complainant must establish that the complainant suffered an adverse action. Courts and OSHA apply the U.S. Supreme Court’s definition of an adverse action set forth in *Burlington Northern and Santa Fe Railway Company v. White*.<sup>34</sup> There, the Court held that adverse actions include those that might “have dissuaded a reasonable worker from [engaging in protected activity].”

To establish a prima facie case, the Secretary must show that:

- The employee engaged in protected activity
- The employer took adverse action against the employee
- A causal connection exists between the two

If the Secretary satisfies this burden, the employer must then articulate a legitimate, non-retaliatory reason for the adverse employment action, at which point the burden shifts back to the Secretary to show that the employer’s explanation is pretextual.

*Did the Complainant Engage in Protected Activity?*

One way to defeat a Section 11(c) claim is to rebut a complainant’s assertion that the complainant engaged in protected activity. Activities protected by Section 11(c) include, but are not limited to, the following:

- Filing occupational safety or health complaints with OSHA or other agencies
- Filing occupational safety or health complaints with management
- Instituting or causing to be instituted any proceeding under or related to the OSH Act

- Providing testimony relating to occupational safety or health
- Exercising any right afforded by the OSH Act
- Refusing to perform a dangerous assigned task under certain circumstances
- Complying with and obtaining benefits of OSHA standards and regulations
- Participating in an OSHA inspection
- Requesting information from OSHA
- Refusing to inform an employer of the identity of the person who complained to or contacted OSHA

In addition, [“O]ccasions might arise when an employee is confronted with a choice between not performing assigned tasks or subjecting himself to serious injury or death arising from a hazardous condition at the workplace,”<sup>30</sup> and, on those occasions, an employer cannot take action against the employee without violating Section 11(c).

Section 11(c) also protects employees whom an employer perceives to have engaged in any of these activities, even if such perception is mistaken, or when an employer retaliates against a person who is closely connected with someone who engaged in protected activity.<sup>31</sup>

<sup>30</sup> 29 C.F.R. § 1977.12(b)(2). <sup>31</sup> See *Cambridgeport Air Sys., Inc.*, 26 F.3d at 1189 (affirming district court’s finding of Section 11(c) liability where complainant “was terminated because of his connection with [another employee who employer believed engaged in protected activity]” where they were “particularly close friends,” management knew they were close friends, a supervisor had warned the plaintiff not to raise safety concerns, and their terminations occurred within one week of each other.”); *Perez v. Lloyd Indus.*, 399 F. Supp. 3d 308, 319 (E.D. Pa. 2019) (holding that complainant need not have actually engaged in protected activity, and “it was sufficient that [respondent’s manager] perceived that [complainant] engaged in a protected activity.”).

<sup>32</sup> See *Marshall v. Springville Poultry Farm, Inc.*, 445 F. Supp. 2d 3 (M.D. Pa. 1977) (holding that an employee’s internal safety complaint to his or her employer is protected under Section 11(c)); *Donovan v. R.D. Andersen Constr. Co., Inc.*, 552 F. Supp. 249, 252 (D. Kan. 1982) (holding that employee’s communications with a newspaper regarding safety conditions in the workplace were protected under Section 11(c)). <sup>33</sup> See *Solis v. Consol. Gun Ranges*, 2011 U.S. Dist. LEXIS 33547, at \*18–19 (W.D. Wash. Mar. 30, 2011) (holding that a manager did not engage in protected activity when he sent an email raising concerns about the company’s handling of lead to save his job and deflect blame when an employee under his supervision had suffered lead poisoning). <sup>34</sup> 548 U.S. 53, 67–68, 126 S. Ct. 2405, 2414–15, 65 L. Ed. 2d 345, 358–59 (2006). <sup>35</sup> *Id.* <sup>36</sup> See *Perez v. U.S. Postal Serv.*, 76 F. Supp. 3d 1168, 1185 (W.D. Wash. 2015) (“Ordinarily, participation in investigative interviews, standing alone, does not constitute punishment or harm sufficient to deter a reasonable employee from engaging in protective activity. Investigative interviews may, however, rise to an actionable level where they lead to an adverse consequence or where the attending circumstances show that a reasonable person subjected to them would be dissuaded from complaining about discrimination.”) (citations omitted). <sup>37</sup> See 29 C.F.R. § 1977.6(b). (“If the discharge or other adverse action would not have taken place ‘but for’ engagement in protected activity, Section 11(c) has been violated.”) (citing *Bostock v. Clayton Cty., Ga.*, 140 S. Ct. 1731, 1739, 207 L. Ed. 2d 218, 232 (2020); *Univ. of Tex. Sw. Med. Ctr. v. Nassar*, 570 U.S. 338, 133 S. Ct. 2517, 186 L. Ed. 2d 503 (2013)). <sup>38</sup> Compare *Perez v. Eastern Awning Sys., Inc.*, 2018 U.S. Dist. LEXIS 173900, at \*28 (D. Conn. Oct. 10, 2018) (“Close temporal proximity between the plaintiff’s protected action and the employer’s adverse employment action may in itself be sufficient to establish the requisite causal connection between a protected activity and retaliatory action.”) (quoting *Kaytor v. Elec. Boat Corp.*, 609 F.3d 537, 552 (2d Cir. 2010)); and *Fairmount Foundry, Inc.*, 2019 U.S. Dist. LEXIS 232592, at \*1, n.1 (“Fairmount argues temporal proximity, standing alone, is never sufficient to show causation in a retaliation claim. This is incorrect. In this circuit, the causal link between protected activity and the adverse employment action may be shown by temporal proximity “unusually suggestive of retaliatory motive.”) (citing *Carvalho-Grevious v. Del. State Univ.*, 851 F.3d 249, 260 (3d Cir. 2017)); with *Dura-Fibre LLC*, 2018 U.S. Dist. LEXIS 89536, at \*22 (“[M]ore than temporal proximity is required to show retaliation.”) (citing *O’Leary v. Accretive Health, Inc.*, 657 F.3d 625, 635 (7th Cir. 2011)); *Chao v. Norse Dairy Sys.*, 2007 U.S. Dist. LEXIS 71478, at \*36 (S.D. Ohio Sept. 26, 2007) (“In [Section 11(c)] retaliation cases, temporal proximity alone is insufficient to establish a causal connection.”).

## Related Content

For additional information on federal and state whistleblower laws and protections, see



**WHISTLEBLOWING STATE AND FEDERAL PRACTICE NOTES CHART**

For a presentation to provide training on handling whistleblower reports to management employees and other key stakeholders in an organization, see



**WHISTLEBLOWER REPORTING: TRAINING PRESENTATION**

For a resource kit focused on employees returning to work and broken up by key employment law topics, see



**CORONAVIRUS (COVID-19) RESOURCE KIT: RETURN TO WORK**

For more guidance on a wide variety of COVID-19 legal issues, see



**CORONAVIRUS (COVID-19) RESOURCE KIT**

For a detailed collection of key federal, state, and local COVID-19-related labor and employment legal developments, see



**CORONAVIRUS (COVID-19) FEDERAL AND STATE EMPLOYMENT LAW TRACKER**

For a summary of the various types of COVID-19 workplace cases that employees have filed against employers, along with an analysis of the frequency of these types of lawsuits to identify current litigation trends, see



**COVID-19 WORKPLACE LITIGATION TRENDS**

There is no bright-line test as to what time period is sufficient to create an inference of causation, and courts will consider the particular circumstances of each case. As a general rule, a temporal proximity of a few hours or days will support an inference of causation, while an intervening period of weeks or months, without other evidence, is likely insufficient.

Another aspect of timing to consider is whether the adverse action occurred before the protected activity. As a matter

of logic, if the adverse action preceded the complainant's protected activity, causation is lacking.<sup>39</sup> Thus, when gathering evidence to defend a Section 11(c) claim it may be useful to ask decisionmakers for notes, emails, calendar and diary entries, and any other evidence that may show when they made their decision to take an adverse action.

Another key element of causation is employer knowledge. A decisionmaker who is unaware that an employee engaged in protected activity cannot retaliate against the employee for such activity. Accordingly, an effective method to defeat causation is to show that the pertinent decisionmakers lacked knowledge of the complainant's protected activity.<sup>40</sup>

Note, however, that proof of actual knowledge is not required, and a complainant may rely on circumstantial evidence or proof that a decisionmaker suspected the complainant engaged in protected activity.<sup>41</sup> Therefore, when investigating and gathering evidence, you should determine exactly when, how, and whether any decisionmakers learned of a complainant's protected activity.

*Establish the Respondent's Legitimate Non-retaliatory Reason for the Adverse Action*

Another effective way to defeat a Section 11(c) claim is to prove that the respondent took an adverse action for a legitimate, non-retaliatory reason. The regulations implementing Section 11(c) state: "An employee's engagement in activities protected by the Act does not automatically render him immune from discharge or discipline for legitimate reasons, or from adverse action dictated by non-prohibited considerations."<sup>42</sup> Thus, an employer can avoid liability by showing that it would have taken the same action in the absence of the complainant's protected activity.

Employers should ensure that any personnel issues or other problems that lead to an adverse action are timely and thoroughly documented. If you intend to use the employer's records to support the defense, you should ensure that the records are consistent with the employer's asserted explanations for the adverse action. Employers should also ensure that they follow all investigation and discipline protocols or be able to explain any deviations from those protocols, to avoid a finding that its asserted reason for taking an adverse action is a pretext for unlawful retaliation.<sup>43</sup>

<sup>39</sup> See *Thomas v. Tyco Int'l Mgmt. Co., LLC*, 416 F. Supp. 3d 1340, 1364 (S.D. Fla. 2019) (holding that, where a plaintiff's negative performance review and other unfavorable personnel actions occurred two months prior to protected activity, "it was not possible for these acts and events to have been made in retaliation for her protected [activity] because that conduct had not yet occurred [and] retaliation can only occur when protected activity precedes retaliation."). <sup>40</sup> See *Perez v. Panther City Hauling, Inc.*, 2014 U.S. Dist. LEXIS 86379, at \*34 (S.D. Ill. June 25, 2014) (denying summary judgment for Secretary of Labor where evidence showed that decisionmakers in plaintiff's termination learned of the complainant's filing of an OSHA complaint after they made the decision to terminate the complainant). <sup>41</sup> See *Reich v. Hoy Shoe Co.*, 32 F.3d 361, 367-68 (8th Cir. 1994) (inferring knowledge where employer suspected that plaintiff had complained to OSHA and holding: "[A]n employer that retaliates against an employee because of the employer's suspicion or belief that the employee filed an OSHA complaint has as surely committed a violation of Section 11(c) as an employer that fires an employee because the employer knows that the employee filed an OSHA complaint."); *Acosta v. Lloyd Indus., Inc.*, 291 F. Supp. 3d 647, 655 (E.D. Pa. 2017) (denying summary judgment on issue of employer knowledge where company owner knew that plaintiff had taken photographs of an unsafe machine that injured another employee shortly before OSHA came to the facility to investigate the machine, because "[c]ommon sense and experience establish that employers also make employment decisions on what they suspect or believe to be true."). <sup>42</sup> 29 C.F.R. § 1977.6(b). <sup>43</sup> See *Dura-Fibre LLC*, 2018 U.S. Dist. LEXIS 89536, at \*25 (holding that employer failed to follow its own accident reporting/investigation procedures when investigating and disciplining plaintiff, which provided evidence of pretext to defeat the employer's assertion of a legitimate, non-retaliatory reason for the adverse action).



To support an employer's legitimate, non-retaliatory reason you should also consider providing evidence that other employees who committed the same infraction as the complainant but did not engage in protected activity were treated the same as the complainant. Evidence that a company has been consistent in its treatment of employees, regardless of protected activity, can be an effective way to establish that the company's asserted reason for an adverse action is genuine.

### COVID-19 and OSH Act Whistleblowing Actions

OSHA whistleblower claims are on the rise since the beginning of the COVID-19 pandemic.<sup>44</sup> On August 14, 2020, the Office of Inspector General of Department of Labor issued a report to OSHA titled: "COVID-19: OSHA Needs To Improve Its Handling Of Whistleblower Complaints During the Pandemic."<sup>45</sup> The report indicated that there was a 30% increase in employee whistleblower complaints filed with OSHA from February 1 through May 31, 2020, during the height of the COVID-19 pandemic. It seems likely that this trend will continue, and may even accelerate, as employees return to work. Meanwhile,

OSHA has stated that it intends to make retaliation complaints a priority, and in April of 2020, it released a statement reminding employers that they may not retaliate against workers for reporting unsafe or unhealthy working conditions relating to COVID-19, signaling that it views employer retaliation as a concern during the pandemic.<sup>46</sup>

On January 21, 2021, President Biden issued an Executive Order that directed OSHA to, among other things, take steps to protect workers who complain about unsafe conditions during the pandemic. On March 12, 2021, OSHA launched a National Emphasis Program (NEP) pursuant to which OSHA's resources will be focused on enforcing the anti-retaliation provisions in Section 11(c). The NEP states that OSHA will do this by "preventing retaliation where possible, distributing anti-retaliation information during inspections, and outreach opportunities, as well as promptly referring allegations of retaliation to the Whistleblower Protection Program." This will likely result in a departure from last year, when OSHA dismissed, without investigation, 54% of the more than 1,700 COVID-19 related complaints it received between April 2020 and August 2020.<sup>47</sup>

<sup>44</sup> See Vin Gurrieri, *OSHA Whistleblower Claims Jump Amid Virus, Watchdog Says*, Law360, Aug. 20, 2020. <sup>45</sup> <https://www.oig.dol.gov/public/reports/oa/2020/19-20-010-10-105.pdf>. <sup>46</sup> U.S. Department of Labor Reminds Employers that They Cannot Retaliate Against Workers Reporting Unsafe Conditions During Coronavirus Pandemic. <sup>47</sup> Braden Campbell, *OSHA Falling Short On COVID-19 Whistleblower Cases*, Law360, Oct. 8, 2020.



It is not surprising that the COVID-19 pandemic has resulted in an increase in whistleblower complaints, since any employee who, in good faith, expresses apprehension about returning to work and contracting COVID-19, or who raises concerns about perceived inadequate PPE or other safety precautions, is likely engaging in protected activity under Section 11(c).

Under 29 C.F.R. § 1977.12(b)(2), an employer may not discipline or discharge an employee who refuses to perform an assigned task because of a reasonable apprehension of death or serious injury, coupled with a reasonable belief that no less drastic alternative is available and insufficient time to eliminate the condition through regular statutory channels. The employee must also have sought and been unable to obtain a correction of the dangerous condition.<sup>48</sup> Thus, whether an employee's refusal to return to work for fear of contracting COVID-19 is protected under 29 C.F.R. § 1977.12(b)(2) and Section 11(c) would depend on the particular facts and circumstances of each case. Relevant factors might include:

- Whether the employee works in crowded areas
- Whether someone else in the workplace tested positive for COVID-19
- Whether proper safety precautions are in place

Given the uptick in retaliation complaints during the COVID-19 pandemic, employers should continue to take employee complaints seriously. Such complaints should be well-documented, and if an employee refuses to work because of COVID-19 fears, employers should engage in an interactive discussion with the employee to understand whether the fear is well-founded before taking any adverse action against the employee.

#### Consider 29 C.F.R. § 1904.35

Employers should also be aware of 29 C.F.R. § 1904.35, which prohibits employers from discriminating or retaliating against

any employee who reports a work-related injury or illness and prohibits employers from creating any policy that would “discourage or deter” an employee from reporting a workplace injury or illness.<sup>49</sup> While Section 11(c) requires an employee to file a complaint, under 29 C.F.R. § 1904.35, OSHA may investigate or cite an employer for a whistleblower violation, with or without an employee filing. Further, unlike the 30-day time limit for filing a Section 11(c) complaint, OSHA has six months to issue a citation under 29 C.F.R. § 1094.35.

While the activity protected by 29 C.F.R. § 1094.35 is more limited than that covered by Section 11(c) in that it only prohibits retaliation for reporting a work-related illness or injury, employers should remember that certain actions might violate both provisions. **■**

**Kenneth D. Kleinman** is senior counsel at Stevens & Lee. He represents management in all areas of employment counseling, employment litigation, and labor relations law. Ken is recognized as one of the leading authorities in occupational safety and health matters and maintains an active national litigation practice. He has successfully negotiated or tried dozens of high-profile, six-figure OSHA citations, including cases involving fatalities, multiple-employer work sites, and criminal prosecutions. He is an editor and chapter author of the nationally recognized treatise, *Occupational Safety and Health Law*, published by the American Bar Association and the Bureau of National Affairs. He is also a former management chair of the ABA Occupational Safety and Health Committee of the Labor and Employment Law Section.

**Brad M. Kushner** is a shareholder at Stevens & Lee. He concentrates his practice in labor and employment matters and has represented clients in class actions and collective actions in courts across the country. Brad counsels employers on OSHA matters and represents employers before the Occupational Safety and Health Review Commission. He is a chapter author for the nationally recognized treatise, *Occupational Safety and Health Law*, published by the American Bar Association and the Bureau of National Affairs. Brad also defends employers against wage and hour claims under the Fair Labor Standards Act and state laws, as well as claims brought under Title VII, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Family Medical Leave Act, and state anti-discrimination laws.

**RESEARCH PATH:** [Labor & Employment > Discrimination, Harassment, and Retaliation > Practice Notes](#)



**Laurie E. Leader** EDITOR-IN-CHIEF, BENDER'S LABOR AND EMPLOYMENT BULLETIN

# Wage and Hour Issues Related to Remote and Hybrid Work: A Fertile Delta for Litigation

Everyone agrees that the COVID-19 pandemic has changed the way we work. Even as pandemic numbers wane, employers have continued to allow remote work schedules and hybrid schedules (some combination of remote and in-person work).

**THIS NEW NORMAL HAS PRESENTED A SLEW OF CHALLENGES** in terms of digital communication, data security and confidentiality concerns, and how employers manage their workforces, maintain productivity, and control off-the-clock work. On the flip side are issues relating to employee isolation and time management.

From a legal standpoint, many of the challenges to remote work revolve around definitions of compensable work and expense reimbursement and whether work that was once exempt from minimum wages and overtime is transformed to non-exempt work in a remote setting.<sup>1</sup> The exemption issue primarily involves commissioned sales employees. At the heart of these challenges lies the Fair Labor Standards Act (FLSA)<sup>2</sup> and the Portal-to-Portal Act<sup>3</sup> at the federal level, as well as state counterpart wage-hour laws.

#### The Statutory Framework

The FLSA generally prescribes minimum wage, overtime, and child labor standards for public agencies and for businesses engaged in commerce and in the production of



<sup>1</sup> Certainly, there are other legal issues to remote work beyond the scope of this article including: who should be allowed to work remotely and whether remote work should be a reasonable accommodation under the Americans with Disabilities Act, administering meal and lunch breaks where required, administering leave and paid time-off policies, and coordinating state wage-hour and leave laws with a multi-state remote workforce. <sup>2</sup> 29 U.S.C.S. § 201 et seq. <sup>3</sup> 29 U.S.C.S. § 251 et seq.

<sup>48</sup> 29 C.F.R. § 1977.12(b)(2). <sup>49</sup> 29 C.F.R. § 1904.35.



goods for commerce, while the Portal-to-Portal Act defines what work is compensable. An employment relationship is one of the benchmarks for statutory coverage. Because the FLSA's definitions of employee and employ offer little guidance in their application, courts were charged with the task of interpreting these terms to determine whether or not an employment relationship exists for coverage purposes.<sup>4</sup> Toward this end, they crafted the economic realities test, a totality-of-the-circumstances test under which courts look to the economic realities of the relationship as a whole.<sup>5</sup>

Most employees are covered by the FLSA. But to determine the wages to which an employee is entitled, the inquiry doesn't stop with a determination of coverage. Covered employees may be exempt from one or more of the statutory requirements.<sup>6</sup> There are numerous exemptions under the FLSA that may be

linked to a particular industry or job category. Exemptions from overtime may be partial or complete. Of particular significance to the issue of remote work is the exemption for outside sales personnel discussed in greater detail below<sup>7</sup>

Assuming coverage and that an employee is nonexempt from a statutory requirement—such as overtime—there is the issue of whether the hours worked are compensable. If so, a covered employee is entitled to be paid 1.5 times his or her regular rate of pay.<sup>8</sup> The employee's regular rate is defined as the employee's hourly rate.<sup>9</sup> There are rules as to how to compute the regular rate, but that is not typically an issue for remote workers. Most often the issues that arise are whether the work performed is compensable and whether an employer must pay for unauthorized overtime.<sup>10</sup>

4. The FLSA defines employee as "any individual employed by an employer." 29 U.S.C.S. § 203(e)(1). Equally unhelpful is the statutory definition of employ defined as "to suffer or permit to work." 29 U.S.C.S. § 203(g). 5. See *Rutherford Food Corp. v. McComb*, 331 U.S. 722, 730, 67 S. Ct. 1473, 1477, 91 L. Ed. 1772, 1778 (1947). 6. The exemptions are set forth in the statute (see generally 29 U.S.C.S. § 213) but defined in the U.S. Department of Labor's regulations (see 29 C.F.R. Pt. 541 for the regulations governing the FLSA's white-collar exemptions). 7. 29 C.F.R. § 541.500. 8. 29 U.S.C.S. § 207(a)(1). 9. 29 C.F.R. § 778.108. 10. Unauthorized overtime generally refers to overtime which the employer challenges as never authorized or of which it was unaware. As discussed herein, if the employer reaped the benefit of the work, it will usually be deemed to be compensable.

Particularly in the minimum wage area, state law requirements are often more favorable than the FLSA—a problem in administration for multi-state employers.

Notably, the FLSA is not preemptive of state law. When viewing the FLSA in conjunction with state law, the law that governs is the law most favorable to the employee.<sup>11</sup> This means that an employer must determine whether the state law requirements for minimum wages and overtime as well as the state exemptions are more or less favorable to the employee in deciding what wages are owed. Particularly in the minimum wage area, state law requirements are often more favorable than the FLSA—a problem in administration for multi-state employers.<sup>12</sup>

#### Payment for Unauthorized Remote Work—The Test Is the Employer's Actual or Constructive Knowledge

As previously noted, the FLSA defines employ as "to suffer or permit to work."<sup>13</sup> Department of Labor regulations generally require an employer to pay employees for all hours worked—suffered or permitted—whether or not requested and including work at home.<sup>14</sup> Essentially if the employer knew or should have known of the work being performed, regardless if scheduled, the work is generally compensable. To determine constructive knowledge, courts consider whether the employer should have acquired knowledge of the hours worked through reasonable diligence.<sup>15</sup>

The FLSA requires an employer to "exercise its control and see that the work is not performed if it does not want it to be performed."<sup>16</sup> It is the employer's burden to prevent work when it is not desired and "[t]he mere promulgation of a rule against such work is not enough. Management has the power to enforce the rule and must make every effort to do so."<sup>17</sup> Accordingly, work that the employer did not request or authorize but suffered or permitted is compensable.<sup>18</sup>

As a practical matter, how do employers avoid paying for unauthorized work, given the difficulty of tracking remote work? One means to do so is "by establishing a reasonable process for an employee to report uncompensated work time."<sup>19</sup> If an employee fails to report hours worked under procedures established for this purpose, the employer is not required to inquire or investigate further to uncover unreported hours.<sup>20</sup>

There are a few caveats to this rule, however. First and foremost, the employer cannot implicitly or explicitly discourage an employee from reporting hours worked and must compensate employees for all reported hours worked.<sup>21</sup> Similarly, if an employer is notified that an employee is working or if employees are not properly instructed on how to report hours under the employer's system, then the employer must pay for the hours worked.<sup>22</sup> Notably, where no reporting system is in place, an employee may be compensated for estimated time spent working off-the-clock.<sup>23</sup>

#### The FLSA's Outside Sales Exemption and Remote Work

The FLSA's outside sales exemption provides a classic case of how remote work may affect an employee's entitlement to minimum wages and overtime. Specifically, the outside sales exemption exempts salespersons from FLSA minimum wage and overtime requirements if they satisfy a duties test, which includes a requirement that the exempt salesperson is "customarily and regularly engaged away from the employer's place or places of business" in "making sales" or in "obtaining orders or contracts for services or for the use of facilities for which a consideration will be paid by the client or customer" as their "primary duty."<sup>24</sup>

11. See generally 29 U.S.C.S. § 218(a) (allowing states to set greater minimum wage, maximum hour, and child labor standards than the FLSA provides). 12. For a state-by-state analysis of wage-hour laws, see 1 Wages & Hours: Law and Practice CHAPTER 13.syn. 13. 29 U.S.C.S. § 203(g). 14. 29 C.F.R. § 785.11-12. 15. See *Allen v. City of Chi.*, 865 F.3d 936, 945 (7th Cir. 2017), cert. denied, 138 S. Ct. 1302 (2018). 16. 29 C.F.R. § 785.13. 17. *Id.* See also *Chao v. Gotham Registry, Inc.*, 514 F.3d 280, 291 (2d Cir. 2008). 18. 29 C.F.R. § 785.11. 19. *Allen*, 865 F.3d at 938. 20. *Id.* See also *White v. Baptist Mem'l Health Care Corp.*, 699 F.3d 869, 876 (6th Cir. 2012) ("When the employee fails to follow reasonable time reporting procedures she prevents the employer from knowing its obligation to compensate the employee"); *Kellar v. Summit Seating Inc.*, 664 F.3d 169, 177 (7th Cir. 2011) ("However, the FLSA stops short of requiring the employer to pay for work it did not know about, and had no reason to know about."). 21. *Allen*, 865 F.3d at 939. 22. *Allen*, 865 F.3d at 946 n.5. 23. See *McDaniel v. Apex Sys.*, 2021 U.S. Dist. LEXIS 250967, at \*\*3-4 (N.D. Cal. May 4, 2021) (plaintiffs stated a claim on behalf of themselves and others similarly situated for alleged failure to be compensated "for all hours worked and off-the-clock work including (a) time spent onboarding before each employee's first shift, (b) during purported 'meal [and rest] breaks'; (c) travelling to mandatory trainings or work-related functions, and (d) remotely logging and reporting hours of work or other administrative tasks"). *McDaniel* also highlights some of the issues related to remote work and expense reimbursement, in this case, for the employer's failure to reimburse employees for business-related costs including the use of personal cell phones to "field work-related calls and texts from Apex representatives" and to receive automated text message reminders to submit time entries. 2021 U.S. Dist. LEXIS 250967, at \*\*9-10. 24. 29 U.S.C.S. § 213(a)(1); 29 C.F.R. § 541.500. The term "making sales" is statutorily defined (29 U.S.C.S. § 203(k)), whereas "primary duty" is defined in the regulations (29 C.F.R. § 541.700).



### Related Content

For an overview of information on defending against federal wage and hour investigations and claims, see

 [WAGE AND HOUR CLAIMS AND INVESTIGATIONS RESOURCE KIT](#)

For coverage of federal, state, and major local employment laws addressing the COVID-19 pandemic, see

 [CORONAVIRUS \(COVID-19\) FEDERAL AND STATE EMPLOYMENT LAW TRACKER](#)

For a summary of the types of COVID-19 workplace cases filed by employees, see

 [COVID-19 WORKPLACE LITIGATION TRENDS](#)

For a resource kit focused on employees returning to work and broken up by key employment law topics, see

 [CORONAVIRUS \(COVID-19\) RESOURCE KIT: RETURN TO WORK](#)

For more guidance on a wide variety of COVID-19 legal issues, see


 [CORONAVIRUS \(COVID-19\) RESOURCE KIT](#)

For a discussion of the FLSA overtime requirement, see

 [OVERTIME REQUIREMENTS FOR HOURLY NON-EXEMPT EMPLOYEES UNDER THE FLSA](#)

In the pandemic environment, many salespersons have been precluded from visiting customers on site. If they are working remotely, their home office may be considered the employer's place of business. Under the circumstances, if they are making sales from their home office, they are engaged in inside sales work rather than in exempt outside sales work. Accordingly, unless they otherwise qualify for an exemption (e.g., as a highly compensated employee), they will need to be paid minimum wages and overtime and will need to be reclassified on a temporary or permanent basis.

### Conclusion

Not only has the pandemic impacted how we work, it has presented a host of legal challenges for employers that are still evolving. In the wage-hour area, these challenges are likely to be the subject matter of litigation. To minimize that risk, employers should establish and clearly communicate in writing that off-the-clock work, underreporting of hours, and unauthorized overtime are strictly prohibited. Managers and supervisors should also be trained on the company's timekeeping and pay policies, so that they can ensure that employees are following them, recording all hours worked, and not seeking to be paid for unnecessary overtime work. 

*Laurie E. Leader, formerly a clinical professor at Chicago-Kent College of Law, is a practicing attorney, author, certified mediator, and principal of Effective Employment Mediation, LLC—Chicago, Northfield, & Libertyville Offices. She has authored numerous articles and book chapters and two treatises and is Editor-in-Chief of Bender's Labor and Employment Bulletin. Laurie earned an A.B. degree from Washington University in St. Louis and her J.D. degree from Cleveland State University.*

 [RESEARCH PATH: Labor & Employment > Trends & Insights > Articles](#)



Jessica D. Bradley JONES DAY

# Expungement and Reexamination Proceedings under the Trademark Modernization Act

This article discusses ex parte expungement and reexamination proceedings at the U.S. Patent and Trademark Office (USPTO).

**SUCH PROCEEDINGS SEEK FULL OR PARTIAL CANCELLATION** of federal trademark registrations that do not meet the use in commerce requirements of the Lanham Act. The article discusses the grounds for each type of petition, procedural considerations including time limits and who can file, requirements for investigating and filing petitions, a registrant's options for proving use or otherwise responding to petitions, and how the USPTO processes and examines the petitions.

The Trademark Modernization Act (TMA), enacted on December 27, 2020, amended the Lanham Act to establish the new expungement and reexamination proceedings. The goal of the proceedings is to foster clearing clutter (i.e., trademarks that are not properly in use in commerce) from the USPTO trademark register that may be blocking legitimate business owners from clearing and registering their marks.<sup>1</sup> Additionally, the proceedings are intended to provide a more efficient and less expensive alternative to a contested Trademark Trial and Appeal Board (TTAB) inter partes cancellation proceeding.<sup>2</sup> While the grounds for expungement and reexamination differ, many of the procedures for instituting the proceedings are largely the



same, including the nature of the evidence and the process for evaluating the petitions and the registrant's response.<sup>3</sup>



## Grounds for Expungement and Reexamination

On December 18, 2021, the USPTO rules governing expungement and reexamination proceedings became effective and the USPTO began accepting petitions. The USPTO issued an examination guide that governs the proceedings until the guidance can be incorporated in the next update of the Trademark Manual of Examining Procedure.<sup>4</sup> Each type of petition is focused on a particular type of nonuse.

### Expungement

A petition for expungement:

- May be filed against any federal trademark registration (i.e., any registration filed under Sections 1, 44, or 66 of the Lanham Act,<sup>5</sup> including registrations for collective and certification trademarks)
- Must identify and establish with evidence that the trademark has never been used in commerce on some or all the goods and/or services covered by the registration<sup>6</sup>

### Reexamination

A petition for reexamination:

- May only be filed against federal trademarks registered under Section 1 of the Lanham Act,<sup>7</sup> including supplemental registrations and registrations for collective and certification trademarks (i.e., it cannot be filed against trademarks registered under §§ 44 or 66)
- Must identify and establish with evidence that the trademark was not in use in commerce on some or all the goods and/or services covered by the registration as of the relevant date:
  - **Use-based trademark application filed under Section 1(a), 15 U.S.C. § 1051(a).** The relevant date is the filing date of the trademark application. If the filing basis of the trademark application is ever later amended to Section 1(b) for any of the goods/services covered in the petition, then the relevant date is that listed below.

- **Intent-to use trademark application filed under Section 1(b), 15 U.S.C. § 1051(b).** The relevant date is the later of:
  - The filing date of an amendment to allege use under Section 1(c),<sup>8</sup> which covers the goods/services that are the subject of the petition
  - The expiration of the deadline for filing a statement of use under Section 1(d),<sup>9</sup> for the goods/services covered by the petition, including all approved extensions of the deadline for filing a statement of use<sup>10</sup>

## Who May File

### Third Parties

Any third-party company or individual may file a petition for expungement or reexamination.<sup>11</sup> You do not have to meet the TTAB requirements for opposition and cancellation proceedings of showing an entitlement to a statutory cause of action (i.e., standing). Additionally, you are not required to identify the actual party with an interest in the proceeding, but can, for example, file a petition in an attorney's name rather than a client's name.<sup>12</sup> You may want to consider this option if you have grounds to believe that the trademark registrant might take action against you in response to a petition. However, the USPTO Director can require the attorney to identify his or her client, (i.e., the real party in interest), such as to discourage and prevent abusive filings.<sup>13</sup>

If the USPTO accepts a petition for expungement or reexamination, then the petitioner's role in the proceeding ends upon issuance of the notice of institution.<sup>14</sup> The remainder of the proceeding is conducted between the USPTO and the registrant. If you prefer a more active role, you may consider filing a cancellation action at the TTAB asserting the new ground of expungement established under the TMA. Expungement requires you show that a registered trademark has never been used in commerce and is available any time after the first three years from the registration date.<sup>15</sup> However, if the registrant contests the TTAB cancellation (i.e., does not default), then the proceeding is likely to be longer and more expensive than a petition for expungement or reexamination.

### USPTO Director

The USPTO Director also may begin an expungement or reexamination proceeding.<sup>16</sup> Director-initiated proceedings are available on the same grounds as third-party petitions and are subject to the same time limits and procedures.<sup>17</sup>

The USPTO Director may also institute an expungement or reexamination against a registration covered by a pending third-party petition for goods/services that are not covered by the third-party petition.<sup>18</sup>

The USPTO considered and rejected a suggestion that it provide an email address for use in notifying the USPTO Director of registrations third parties believed were vulnerable to a Director-initiated expungement or reexamination proceeding.<sup>19</sup> Where a third party believes grounds exist for expungement or reexamination the proper procedure for notifying the USPTO is for that third party to file such a petition.<sup>20</sup>

### Trademark Registrants Prohibited from Filing against Own Registration

Trademark registrants cannot file a petition for expungement or reexamination against their own trademark registrations.<sup>21</sup> If there are goods or services in your own registrations that are not in use, then you should file either:

- An amendment to delete the goods or services that are not in use (or were never in use)
- A surrender of the registration for cancellation if none of the goods or services are in use (or were never in use)<sup>22</sup>

## Time Limits for Filing a Petition

### Expungement

A petition for expungement may be filed against any federal trademark registration during the following time periods:

- **Until December 27, 2023.** A petition may be filed against any registration that is three years or older.
- **After December 27, 2023.** A petition may be filed against a registration between years three to ten following the registration date.<sup>23</sup>

Given the limited exception until December 27, 2023, consider reviewing the register for any existing registrations that could present an issue for your client's current or future marketing plans. If you can establish the required lack of use you may want to file a petition to clear any potentially blocking registration before the limited exception expires.

### Reexamination

A petition for reexamination may be filed against any trademark registered under Section 1<sup>24</sup> in the first five years following the registration date.<sup>25</sup>

<sup>4</sup> See USPTO Examination Guide 1-21, Expungement and Reexamination Proceedings Under the Trademark Modernization Act of 2020 (Dec. 2021) (Examination Guide 1-21). <sup>5</sup> 15 U.S.C.S. §§ 1051, 1126, 1141f. <sup>6</sup> 15 U.S.C.S. § 1066a(a); 37 C.F.R. §§ 2.91(a)(1), 2.92(g). <sup>7</sup> 15 U.S.C.S. § 1051.

<sup>8</sup> 15 U.S.C.S. § 1051(c). <sup>9</sup> 15 U.S.C.S. § 1051(d). <sup>10</sup> 15 U.S.C.S. § 1066b(a)-(b), (k); 37 C.F.R. §§ 2.91(a)(2), 2.92(g). <sup>11</sup> 15 U.S.C.S. §§ 1066a(a), 1066b(a). <sup>12</sup> 86 Fed. Reg. 64308. <sup>13</sup> 37 C.F.R. §§ 2.91(h). <sup>14</sup> Examination Guide 1-21, at p. 7. <sup>15</sup> 15 U.S.C.S. § 1064(6). <sup>16</sup> 15 U.S.C.S. §§ 1066a(h), 1066b(h); 37 C.F.R. § 2.92(b). <sup>17</sup> *Id.* <sup>18</sup> 37 C.F.R. § 2.92(c)(2). <sup>19</sup> 86 Fed. Reg. 64311. <sup>20</sup> *Id.* <sup>21</sup> 86 Fed. Reg. 64301. <sup>22</sup> 15 U.S.C.S. § 1057(e). <sup>23</sup> 15 U.S.C.S. § 1066a(i); 37 C.F.R. § 2.91(b)(1). <sup>24</sup> 15 U.S.C.S. § 1051. <sup>25</sup> 15 U.S.C.S. § 1066b(i); 37 C.F.R. § 2.91(b)(2).



The TMA requires that petitions for expungement and reexamination include the results of a reasonable investigation. It must be “a bona fide attempt to determine if the registered mark was not in use in commerce or never in use in commerce on or in connection with the goods and/or services” identified in the petition.

### Contents of a Petition for Expungement or Reexamination

A petition for expungement or reexamination must be in writing, filed through the USPTO Trademark Electronic Application System, and contain the following elements:

- **Fee.** The fee to file a petition is \$400 per international class.<sup>26</sup>
- **Petitioner.** Identify the petitioner’s name, domicile address, and email address. The petitioner identified does not need to be the real party in interest, but the USPTO Director can require this identity where needed.<sup>27</sup> Additionally:
  - If the petitioner’s domicile is not within the United States or its territories, then the petition must designate a qualified U.S.–licensed attorney.<sup>28</sup>
  - If the petitioner must be represented by an attorney, then include the attorney’s name, postal address, email address, and bar information.<sup>29</sup>
- **U.S. trademark registration.** List the U.S. trademark registration number for the registration being challenged. Only one registration number can be listed per petition.<sup>30</sup>
- **Basis.** Identify either expungement or reexamination as the basis for the petition. It is not possible to assert both expungement and reexamination in a single petition.<sup>31</sup>
- **Goods and/or services challenged.** Identify each good and/or service covered by the registration that is challenged in the petition.
- **Verified statement of reasonable investigation.** The verified statement must:
  - Be signed by someone with firsthand knowledge of the facts
  - List the facts in numbered paragraphs
  - Identify the elements of the reasonable investigation of nonuse conducted including:
    - List each source of information petitioner relied upon
    - Describe how and when petitioner conducted each search in its investigation
    - Describe what each search showed<sup>32</sup>

- List each source of information petitioner relied upon
  - Describe how and when petitioner conducted each search in its investigation
  - Describe what each search showed<sup>32</sup>
  - Contain a concise statement describing the relevant factual basis for the petition and any additional facts supporting the allegation of nonuse
- **Documentary evidence of nonuse.** Include a clear and legible copy of all supporting documentary evidence of nonuse and a correlating itemized index of such evidence.<sup>33</sup>

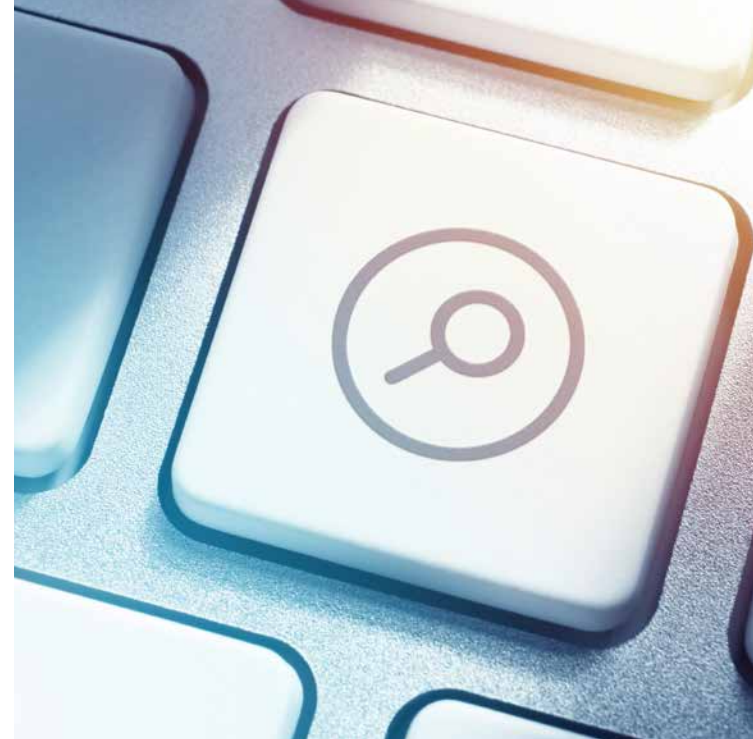
### Reasonable Investigation

The TMA requires that petitions for expungement and reexamination include the results of a reasonable investigation. It must be “a bona fide attempt to determine if the registered mark was not in use in commerce or never in use in commerce on or in connection with the goods and/or services” identified in the petition.<sup>34</sup> The USPTO defines a reasonable investigation as:

[A]n appropriately comprehensive search, which may vary depending on the circumstances but is calculated to return information about the underlying inquiry from reasonably accessible sources where evidence concerning use of the mark during the relevant time period on or in connection with the relevant goods and/or services would normally be found.<sup>35</sup>

What will constitute a reasonable investigation is a case-by-case determination depending on:

- The goods and/or services at issue
- The relevant industry and marketplace for such goods and/or services
- The normal trade channels and advertising for such goods and/or services<sup>36</sup>



For example, “evidence of sales of a large, specialized commercial product may not be returned by the results of internet searches and may require additional efforts to satisfy the showing needed to establish a prima facie case.”<sup>37</sup> Additionally, in a recent Director–initiated expungement proceeding involving a registration covering consumer goods like floor coverings and gymnastics mats owned by a foreign registrant, the USPTO found it would be “reasonable to expect that if the mark were used in U.S. commerce, the registrant would have an internet presence and references to the mark would be found through searches of internet sources where goods of the type are traditionally sold.”<sup>38</sup> The USPTO’s evidence included:

- Searches of several websites where the types of goods are traditionally sold including Amazon, Home Depot, Lowe’s, Walmart, Dick’s Sporting Goods, and US Gym Products
- Google searches for the trademark and the registrant
- Wayback Machine searches for the mark and the registrant<sup>39</sup>

The lack of hits for any products on the online retail sites and the lack of references to the registrant or its mark in the general internet searches both supported a prima facie case of nonuse.

The relevant use of the trademark for the investigation is that consistent with use in commerce as defined in the Lanham Act, (i.e., “bona fide use of a mark in the ordinary course of trade, and not made merely to reserve a right in a mark”).<sup>40</sup>

Consider the following guidelines in meeting the reasonable investigation standard:

- Searches should be comprehensive enough to cover the most likely sources of where goods and/or services would be expected to be sold and advertised, but you do not need to check every possible source.<sup>41</sup>
- A search should “encompass the relevant online sources that would be searched and returned if it was conducted by someone seeking information about a product or service that is in use in commerce.”<sup>42</sup>
- A review of pages from a single website, or a single search using an internet search engine, is generally not considered a reasonable investigation.<sup>43</sup>
- An investigation consisting only of a review of registrant’s portfolio of marks on the USPTO register and a review of the registrant’s website is likely insufficient.<sup>44</sup>
- An investigation conducted by a private investigator is not required or expected, but the results of any such investigation may be referenced.<sup>45</sup>
- Current evidence of nonuse is insufficient. The investigation must also include evidence documenting past nonuse.<sup>46</sup>
- For a petition involving a design mark consider conducting a reverse image search.<sup>47</sup>

The petitioner must submit the results of its reasonable investigation through both a verified statement and documentary evidence of nonuse.<sup>48</sup>

### Verified Statement

The verified statement of reasonable investigation must:

- Be signed by someone with firsthand knowledge of the facts
- List the facts in numbered paragraphs
- Identify the elements of the reasonable investigation of nonuse conducted including:
  - Each source of information petitioner relied upon
  - How and when petitioner conducted each search in its investigation
  - What each search showed<sup>49</sup>
- Contain a concise statement describing the relevant factual basis for the petition and any additional facts supporting the allegation of nonuse<sup>50</sup>

26. 37 C.F.R. § 2.6(a)(26). 27. 37 C.F.R. § 2.91(h). 28. 8 Trademark Manual of Examining Procedure § 601. 29. 37 C.F.R. § 2.17(b)(3). 30. Examination Guide 1-21, at p. 3. 31. *Id.* 32. 37 C.F.R. § 2.91(d). 33. 15 U.S.C.S. §§ 1066a(b), 1066b(c); 37 C.F.R. § 2.91(c); Examination Guide 1-21, at p. 4. 34. 15 U.S.C.S. §§ 1066a(b)(3)(A); 1066b(c)(3)(A). 37 C.F.R. § 2.91(d). 35. 37 C.F.R. § 2.91(d)(1). 36. 86 Fed. Reg. 64302; Examination Guide 1-21, at p. 5.

37. H.R. Rep. No. 116-645, at 15 (2020). 38. See Trademark Status & Document Retrieval (TSDR) record for U.S. Registration No. 5513424. 39. *Id.* 40. 15 U.S.C.S. § 1127; see also 8 Trademark Manual of Examining Procedure § 901. 41. See 37 C.F.R. § 2.91(d)(2)(viii). 42. 86 Fed. Reg. 64310. 43. See H.R. Rep. No. 116-645, at 15. 44. See TSDR record for U.S. Registration No. 5527146. 45. 86 Fed. Reg. 64303. 46. Examination Guide 1-21, at p. 5. 47. See USPTO presentation, Insights into Trademark Modernization Act Nonuse Cancellation Petitions (Slide 10). 48. 37 C.F.R. § 2.91(c)(8)-(9). 49. 37 C.F.R. § 2.91(d). 50. 37 C.F.R. § 2.91(c)(8).



For example, for internet searches you should include a description of the following in the verified statement:

- The website that was searched
- The search term(s) that you used
- The date the search was conducted
- The results of the search (i.e., no hits returned or only hits returned were for irrelevant third parties, etc.)

A verified statement must be corroborated by documentary evidence of nonuse.<sup>51</sup>

#### Documentary Evidence of Nonuse

You should submit documentary evidence supporting all statements in the verified statement. For example, if the verified statement states that you ran internet searches that returned no hits, capture and submit screenshots showing these results.<sup>52</sup>

#### Documentary Evidence: Sources

Appropriate sources of documentary evidence should be reasonably accessible sources that can be publicly disclosed.<sup>53</sup> Such sources may include, but are not limited to:

- **USPTO record for the challenged registration.** This is automatically of record in the proceeding, but if there are particular parts of the record that you would like to highlight, then attach it as evidence to your petition.<sup>54</sup>
- **Third-party USPTO applications or registration records.** Include the specific documents from within the third-party

USPTO record that are relevant to the alleged nonuse. Do not simply file the entirety of the USPTO record or just a listing of the prosecution history.

- **State trademark records.**
- **Registrant’s website(s), social media sites, and/or other media believed to be owned or controlled by the registrant.**
- **Registrant’s marketplace activities.** This could include any attempts to contact the registrant and to purchase any goods and/or services.
- **Registrant’s fake, digitally altered, or otherwise insufficient specimen(s) of use.** Generally, an issue with a specimen of use will only be sufficient to show nonuse for the particular good and/or service depicted in the specimen. It will not be sufficient on its own to establish expungement or reexamination for the entire class of goods and/or services.
- **Third-party websites, social media sites, or other online media.** In particular, any sites where the goods and/or services at issue would be likely to be advertised or offered for sale.
- **Search engine searches.**
- **Internet Archive (Wayback Machine) screenshots.** Such screenshots are effective in showing past nonuse, but make sure to capture the date range reflected in the screenshots.

- **Press releases, news articles, journals, magazines, or other publications.** In particular, those where the goods and/or services at issue would be likely to be reviewed or discussed.
- **Litigation or administrative proceedings records.**
- **Federal or state business registration or regulatory filings or actions.**<sup>55</sup>

#### Documentary Evidence: Format

In addition to collecting evidence from appropriate sources, the following tips will increase the effectiveness of your evidence:

- Do not shrink screen captures when collecting screenshots from websites
- Make sure all internet screenshots have legible URLs and access or print dates
- Avoid data dumps by only including the relevant documents or portions of the documents (e.g., do not submit entire trademark registration records)
- For publications, include both the publication name and the date of publication
- Make sure all submitted evidence is legible<sup>56</sup>

#### Index of Evidence

The USPTO requires you to submit an itemized index of all the documentary evidence.<sup>57</sup> Do not just list the exhibits. Instead, the index should:

- Be on its own separate page
- Include an identifier for each exhibit (i.e., Exhibit A or 1) that is used in and correlates to the corresponding discussion in the verified statement and petition
- Identify and explain for each exhibit which goods and/or services the specific exhibit is relevant to showing and/or supporting nonuse<sup>58</sup>

In the initial set of petitions filed with the USPTO, the failure to include the index of evidence was one of the most common mistakes. Including a well-organized index of evidence that identifies each piece of evidence and connects it to the specific goods and/or services at issue will increase the chances of your petition being accepted provided you have sufficient evidentiary support.

For information on filing procedures, petition review, records, and responding to a petition, [follow this link](#) to read the full practice note in Practical Guidance. **L**

### Related Content

For an overview of opposition and cancellation proceedings before the Trademark Trial and Appeal Board (TTAB) of the U.S. Patent and Trademark Office (USPTO), see

 [TTAB PROCEEDINGS RESOURCE KIT](#)

For a discussion on the key changes to trademark law contained in the Trademark Modernization Act of 2020, see

 [TRADEMARK MODERNIZATION ACT OVERVIEW](#)

For guidance on representing clients at trademark cancellation proceedings at the TTAB, see

 [TTAB LITIGATION: CANCELLATION PROCEEDINGS](#)

For a collection of resources on trademark searching and clearance, including Practical Guidance practice notes, templates, and checklists, see

 [TRADEMARK SEARCHING AND CLEARANCE RESOURCE KIT](#)

For an analysis of the requirement to prove that a defendant used a trademark in interstate commerce in order to establish a trademark infringement claim, see

 [1 GILSON ON TRADEMARKS § 3.03](#)

For comprehensive information on key trademark law principles, see

 [TRADEMARK FUNDAMENTALS](#)

*Jessica D. Bradley is a former partner at Jones Day. Jessica has more than 15 years of experience litigating trademark, trade dress, false advertising, unfair competition, dilution, and copyright cases. She also counseled clients on trademark clearance, prosecution, and enforcement, and represented clients before the TTAB.*

 [RESEARCH PATH: Intellectual Property > Trademarks > Practice Notes](#)

51. 37 C.F.R. § 2.91(c)(9). See USPTO presentation, *Insights into Trademark Modernization Act Nonuse Cancellation Petitions* (Slide 10). 52. See USPTO guidance on best practices at USPTO implements the Trademark Modernization Act. 53. Examination Guide 1-21, at p. 5. 54. See 37 C.F.R. § 2.92.

55. See 37 C.F.R. § 2.91(c)(9), (d)(2); USPTO guidance on limitations of proceedings and best practices at USPTO implements the Trademark Modernization Act. 56. See 37 C.F.R. § 2.91(c)(9)(iii)-(iv); USPTO guidance on limitations of proceedings and best practices on the USPTO website. 57. 37 C.F.R. § 2.91(c)(9). 58. See USPTO guidance on best practices at USPTO implements the Trademark Modernization Act. For a good example of an index of evidence, see the Director-initiated proceeding in the TSDR record for U.S. Trademark Registration No. 6372057 (at p. 3-4).

The Practical Guidance Civil Litigation Team

# Civil Litigation Process Map: Pre-litigation (Federal)

This process map resource kit provides an overview of the key stages in the lifecycle of a typical federal court litigation, as well as comprehensive resources providing step-by-step guidance on the most common tasks associated with the pre-litigation phase that you will typically work on in your litigation, including detailed practice notes, annotated templates, and checklists.

WHILE NOT EVERY LITIGATION IS IDENTICAL, MOST FEDERAL court litigations follow the same general lifecycle. The process map below provides a visualization of this lifecycle starting with the pre-litigation phase through final judgment and appeal.

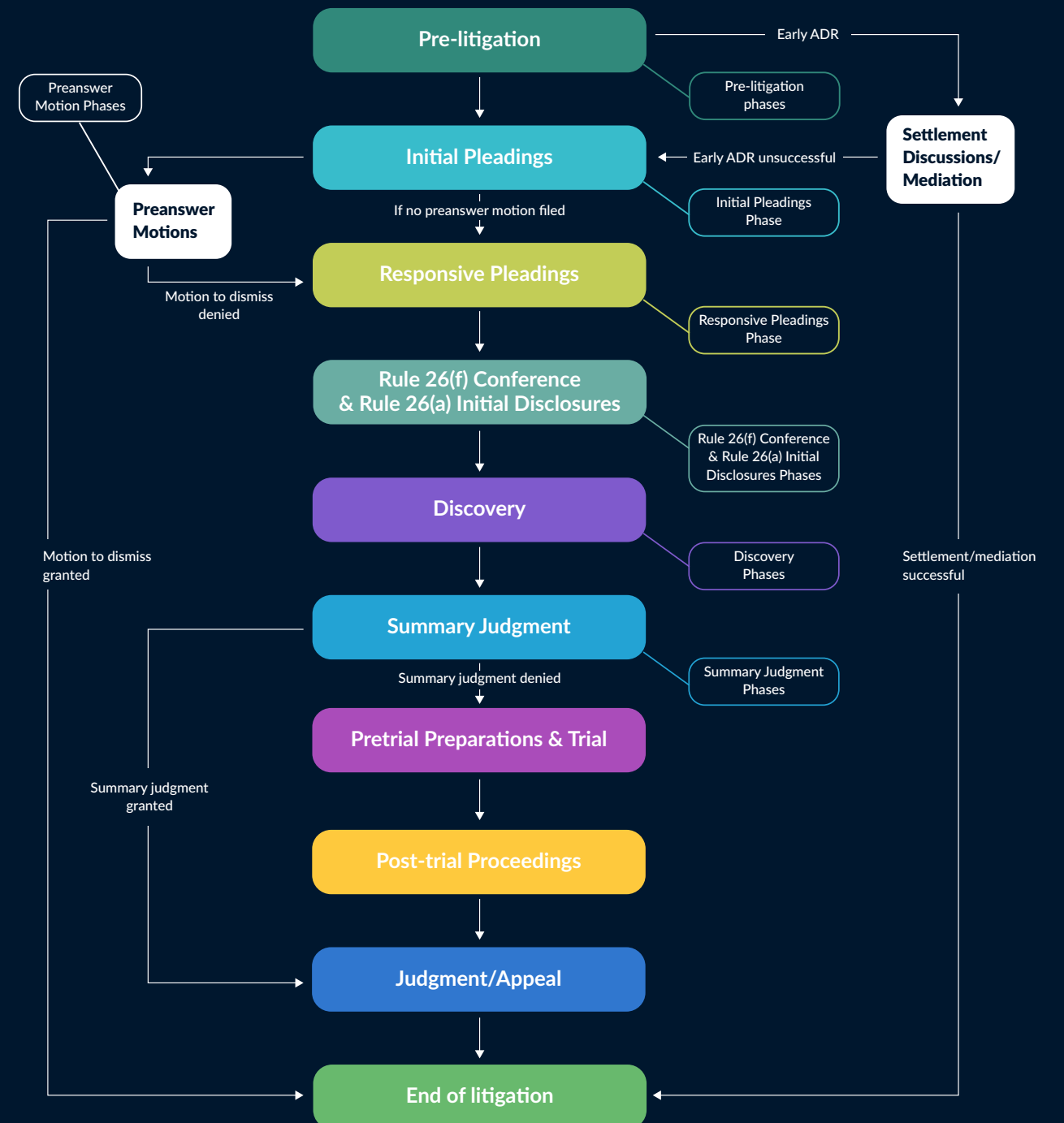
Many of these lifecycle stages have multiple phases covering critical tasks you will typically work on in your federal court litigation.

For practical guidance on other stages and associated tasks throughout the litigation lifecycle, see:

- [Civil Litigation Process Map: Initial Pleadings \(Federal\)](#)
- [Civil Litigation Process Map: Settlement Discussions and Mediation \(Federal\)](#)
- [Civil Litigation Process Map: Preanswer Motions \(Federal\)](#)
- [Civil Litigation Process Map: Responsive Pleadings \(Federal\)](#)
- [Civil Litigation Process Map: Rule 26\(f\) Conference and Rule 26\(a\) Initial Disclosures \(Federal\)](#)
- [Civil Litigation Process Map: Discovery \(Federal\)](#)
- [Civil Litigation Process Map: Summary Judgment \(Federal\)](#)
- [Civil Litigation Process Map: Pretrial Preparations and Trial \(Federal\)](#)



## Litigation Process Map





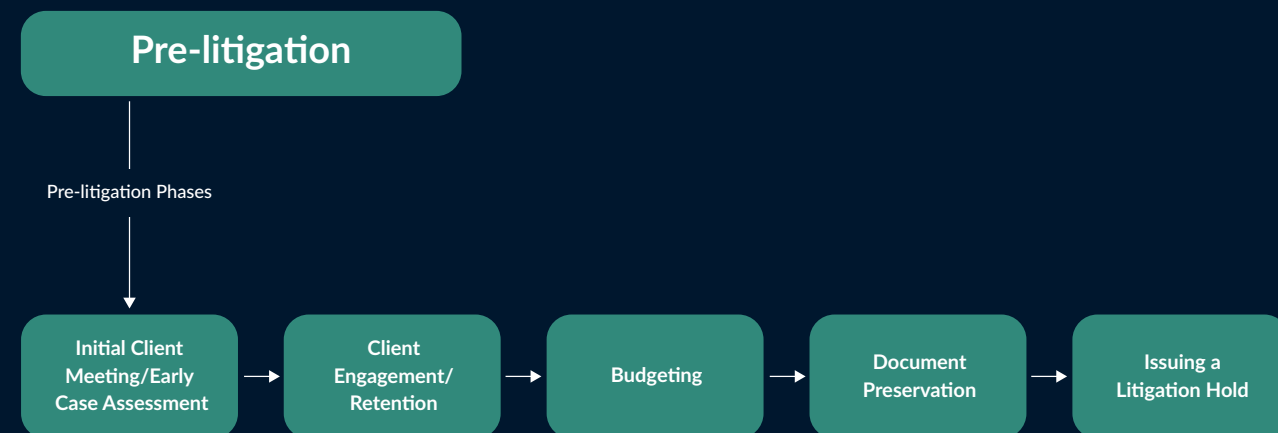
To review previous editions of the Practical Guidance Journal, follow [this link](#) to the archive.

### Pre-litigation

The pre-litigation stage of your federal court litigation will likely include the following phases:

- Initial client meeting/early case assessment
- Client engagement and retention
- Budgeting
- Document preservation
- Issuing a litigation hold

## Pre-litigation Phases



### Initial Client Meeting/Early Case Assessment

The initial client interview is a vital first step in assessing the strength of a potential case and informs the retention decision from both the client's and lawyer's perspectives. At its conclusion, the interview will underscore the eventual framing and assessment of the litigation itself.

The following Practical Guidance resources will guide you through the initial client meeting and early case assessment phase of the pre-litigation stage of your federal court litigation.

| Practical Guidance Documents  | Practical Guidance Content Type |
|---|---------------------------------|
| <a href="#">Commencing a Lawsuit: Evaluating Whether to File Suit (Federal)</a> | Practice Note                   |
| <a href="#">Client Evaluation Checklist (Plaintiff) (Federal)</a>               | Checklist                       |
| <a href="#">Case Evaluation Checklist (Federal)</a>                             | Checklist                       |
| <a href="#">Conflicts Check Checklist (Federal)</a>                             | Checklist                       |
| <a href="#">Client Intake Form (Federal)</a>                                    | Form                            |

### Client Engagement/Retention

After meeting with the prospective client and evaluating the case, you must decide whether you will enter into a formal attorney-client relationship with that prospective client. If you agree to take on the litigation, you and the client must execute an engagement letter formalizing, among other things, the precise scope of the contemplated legal work. If you decide to decline representation, consider sending a non-engagement letter to formally notify the potential client of your decision.

The following Practical Guidance resources will guide you through the client engagement and retention phase of the pre-litigation stage of your federal court litigation.

| Practical Guidance Documents   | Practical Guidance Content Type |
|--|---------------------------------|
| <a href="#">Attorney Engagement Letter and Fee Agreement Checklist (Federal)</a> | Checklist                       |
| <a href="#">Attorney Engagement Letter and Fee Agreement (Federal)</a>           | Form                            |
| <a href="#">Client Conflict Waiver Letter (Current/Former Client) (Federal)</a>  | Form                            |
| <a href="#">Client Conflict Waiver Letter (Prospective Client) (Federal)</a>     | Form                            |
| <a href="#">Attorney Non-engagement Letter (Federal)</a>                         | Form                            |

## Budgeting

Preparing a litigation budget ensures transparency in attorney–client relationships and requires an attorney to think holistically about his or her litigation strategy in a given case. Budgeting takes into consideration each phase of the litigation and the projected number of hours each timekeeper will spend on each task.

As part of the budgeting phase, you may also encounter the growing presence of for–profit investments in federal litigation. Litigation financing involves third–party financiers and companies investing in a case in exchange for a share of any settlement or judgment in favor of the plaintiff. This also includes a pre–agreed sharing of a contingency fee as a payment for the funds advanced to finance the litigation.

The following Practical Guidance resources will guide you through the budgeting phase of the pre–litigation stage of your federal court litigation.

| Practical Guidance Documents                               | Practical Guidance Content Type |
|--|---------------------------------|
| <a href="#">Third-party Litigation Financing (Federal)</a> | Practice Note                   |
| <a href="#">Budget for Litigation (Federal)</a>            | Form                            |

## Document Preservation

Document preservation is a critical phase of any federal court litigation. When a party knows that evidence under its control is relevant to pending litigation or should know that evidence may be relevant to future litigation, the party has an obligation to preserve that evidence.<sup>1</sup> Breach of the duty to preserve relevant evidence with a culpable state of mind gives rise to spoliation.

The following Practical Guidance resources will guide you through the document preservation phase of the pre–litigation stage of your federal court litigation.

| Practical Guidance Documents   | Practical Guidance Content Type |
|--|---------------------------------|
| <a href="#">Electronically Stored Information: Preserving ESI (Federal) – Establishing a Document Retention and Destruction Policy</a> | Practice Note                   |
| <a href="#">Document Retention Policy Presentation (Federal)</a>   | Practice Note                   |
| <a href="#">Preserving Evidence (Federal)</a>  | Practice Note                   |
| <a href="#">Preserving Evidence Video (Federal)</a>  | Practice Note                   |
| <a href="#">Spoliation of Evidence Video (Federal)</a>   | Practice Note                   |
| <a href="#">Electronically Stored Information: Preserving ESI (Federal)</a>  | Practice Note                   |
| <a href="#">Preserving Evidence Checklist (Federal)</a>  | Checklist                       |
| <a href="#">Document Retention Policy Checklist (Federal)</a>  | Checklist                       |
| <a href="#">Document Retention Policy (Federal)</a>  | Form                            |
| <a href="#">Document Preservation Demand Letter (Federal)</a>  | Form                            |

<sup>1</sup> *Silvestri v. GMC*, 271 F.3d 583, 591 (4th Cir. 2001); *Kronisch v. United States*, 150 F.3d 112 (2nd Cir. 1998).



## Issuing a Litigation Hold

A litigation hold is an organization’s written instructions to its employees to preserve documents and information in their possession, custody, or control relevant to a pending or anticipated lawsuit to ensure that the organization complies with its preservation duties. The purpose of the hold is to ensure that the materials in question will be available for future discovery in the litigation.

Once the duty to preserve is triggered, a party organization generally must:

- Suspend its routine document retention/destruction policy
- Put in place a litigation hold to ensure the preservation of relevant documents under its control<sup>2</sup>

The following Practical Guidance resources will guide you through the litigation hold phase of the pre–litigation stage of your federal court litigation

| Practical Guidance Documents   | Practical Guidance Content Type |
|--|---------------------------------|
| <a href="#">Electronically Stored Information: Preserving ESI (Federal) – Litigation Hold Notice</a> | Practice Note                   |
| <a href="#">Litigation Holds 101 Presentation (Federal)</a>  | Practice Note                   |
| <a href="#">Litigation Hold Notice Checklist (Federal)</a>   | Checklist                       |
| <a href="#">Litigation Hold Notice (Federal)</a>   | Form                            |
| <a href="#">Litigation Hold Reminder (Federal)</a>   | Form                            |
| <a href="#">Litigation Hold Escalation Letter (Federal)</a>  | Form                            |
| <a href="#">Litigation Hold Lift Notice (Federal)</a>  | Form                            |

<sup>2</sup> *Orbit One Communs. v. Numerex Corp.*, 271 F.R.D. 429, 437 (S.D.N.Y. 2010).



Erin M. Estevez, Jeremy D. Burkhart,  
and Kelsey M. Hayes

HOLLAND & KNIGHT LLP

# Timing Is Everything: The Impact of Transactions on Pending Bids and Proposals

Recent decisions from the Government Accountability Office (GAO) and the U.S. Small Business Administration's (SBA) Office of Hearings and Appeals (OHA) illustrate the real-world impact that transactions can have on an ongoing procurement and provide practical insight into how contractors can mitigate those risks. The authors of this article discuss the decisions and their implications.

**TO WHAT EXTENT DOES A COMPLETED OR IMMINENT corporate transaction affect a government contractor's ability to compete for award of an opportunity in its pipeline? What steps can a contractor take to prevent a contemplated transaction from negatively impacting its eligibility for or evaluation with respect to a pending bid?** Recent decisions from the GAO and the OHA illustrate the real-world impact that transactions can have on an ongoing procurement and provide practical insight into how contractors can mitigate those risks.

## Can a Transaction Impact Evaluation of an Offeror's Pending Bid for an Award?

In two recent bid protest decisions, the GAO came to opposite conclusions regarding whether a procuring agency properly considered the impact that the same corporate transaction would have on pending procurements.

In *Vertex Aerospace, LLC*,<sup>1</sup> the GAO found the agency's evaluation unreasonable because it failed to adequately



consider the impact of the awardee's recent acquisition by another entity, but in *PAE Aviation and Technical Services, LLC*,<sup>2</sup> the GAO found the agency had properly concluded that the same transaction did not appear likely to impact performance, begging the question of what the key difference was in the conduct of the procurement that led to the contrast in outcomes.

In *Vertex*, the U.S. Air Force had awarded the Aircraft Maintenance Enterprise Solutions (ACES) multiple-award indefinite delivery/indefinite quantity (IDIQ) contract for aircraft maintenance services to eight contractors.<sup>3</sup>

On November 20, 2020, through a series of corporate transactions, one of those contractors became the immediate parent company of another.<sup>4</sup> Nearly a month later, the agency issued a task order solicitation to holders of the ACES IDIQ contract.

During evaluation, the contracting officer received notice of the November 2020 acquisition by virtue of a related novation request.<sup>5</sup> However, the agency did not analyze whether the acquisition would impact the relevant offeror's ability to perform consistent with its task order proposal or, at the very least, the contemporaneous evaluation record did not address the potential ramifications. The agency ultimately concluded that offeror's proposal represented the best value and issued the award accordingly.

*Vertex* protested, contending that the agency's evaluation of proposals was unreasonable and that the agency failed to adequately consider the potential impact of the awardee recently being acquired by another firm. The GAO ultimately sustained the protest because "the record contained insufficient documentation and analysis . . . to conclude that the agency meaningfully and reasonably considered the effect of this corporate transaction on the awardee's ability to perform the task order."<sup>6</sup>

However, just months earlier, in *PAE Aviation and Technical Services*, the GAO was faced with a nearly identical issue arising out of the same transaction as was at issue in *Vertex* but reached a different conclusion.

In *PAE*, the protester challenged a U.S. Customs and Border Protections (CBP) award for aviation logistics and support.<sup>7</sup> Among other arguments, the protester contended that the awardee failed to inform CBP of its pending acquisition and that CBP unreasonably evaluated the awardee's technical and cost proposal due to the transaction.<sup>8</sup> Unlike in *Vertex*, the agency considered the transaction during the evaluation and documented that analysis.

While CBP was performing its responsibility determination of the awardee, the agency learned through public reports that the awardee had been acquired.<sup>9</sup> After CBP's procurement team saw that the awardee was still registered in the System for Award Management with the same data universal numbering system number, CBP concluded that "there was no indication that this new ownership changes [the awardee]'s corporate structure or will have an impact on its ability to perform as proposed." This determination was included in the contracting officer's contemporaneous documentation.<sup>10</sup>

The GAO ultimately denied the protest, stating that "the record provides no basis to find that the transaction will have a significant impact on contract performance."<sup>11</sup>

In the *Vertex* decision, the GAO specifically distinguished *PAE*, noting that in *PAE*, the agency made an explicit pre-award determination that the transaction would not adversely impact that procurement and then documented that decision.<sup>12</sup> This was considered a contemporaneous finding that was given due deference by the GAO.<sup>13</sup>

However, in *Vertex*, because there was no contemporaneous documentation, the GAO had "insufficient information from which to assess the adequacy and reasonableness of the agency's consideration of the effect of the corporate transaction" and thus sustained the protest.

## Key Takeaways from PAE and Vertex

The key takeaway from these two decisions is that contractors must understand their obligations for notification and the government's need to adequately document the details of the transaction.

First, if an offeror is in the process of a corporate transaction, that offeror should include a description of the transaction in any proposals it submits and notify the procuring agency for any already-pending bids as soon as practicable. At the latest, this notification should be made immediately upon the transaction's closing. Notice of the transaction provides an offeror with two advantages: (1) the opportunity to assert that the transaction will not impact performance (cost or technical) and (2) an impetus to the agency to consider this issue and document its determination in the course of its evaluation.

This is the second key, documentation. If an offeror does these things, it minimizes the chance that an eventual award can be successfully protested. Careful attention to pending and pipeline bids during the planning and execution stages of a transaction is merited for these reasons.

1. B-420073, B-420073.2, Nov. 23, 2021, 2022 CPD ¶ 5.

2. B-417704.7, B-417704.8, June 8, 2021, 2021 CPD ¶ 293. 3. *Vertex*, 2022 CPD ¶ 5 at 1. 4. *Id.* 5. *Id.* at 5-6. 6. *Id.* at 11. 7. *PAE*, 2021 CPD ¶ 293 at 1. 8. *Id.* at 1-2. 9. *Id.* at 14. 10. *Id.* 11. *Id.* at 15. 12. *Vertex*, 2022 CPD ¶ 5 at 21-22. 13. *Id.* at 22.



The takeaway from these decisions is that early planning for a contemplated transaction is critical. A transaction could impact eligibility for a set-aside award depending on (1) the timing and (2) how the opportunity is being procured.

### What Impact Does a Transaction Have on a Small Business Offeror's Certification and Recertification Obligations?

What if a pending procurement is a set aside and the corporate transaction will result in the offeror becoming other than small? In general, under SBA's certification rules, a business's size is determined as of the date of its initial offer, including price. Thus, as long as the firm is small at that time, it will be considered small throughout the life of the contract, including (with exceptions) orders issued under multiple-award contracts (MACs). However, if a business goes through a corporate transaction, such as a merger, sale, or acquisition, or novates its small business contract, it is required to recertify its size status pursuant to FAR 52.219-28,<sup>14</sup> Post-Award Small Business Program Representation, and 13 C.F.R. § 121.404.

Revisions to SBA's regulations that became effective in late 2020 now require small businesses with pending bids and proposals to recertify their size status if an acquisition occurs after bid or proposal submission but prior to contract award. Whether the small business will remain eligible to receive a pending award depends on two primary factors: timing and the nature of the procurement. With respect to timing, if the merger, sale, or acquisition occurs within 180 days of the date of an offer and the offeror is unable to recertify as small, it will not be eligible as a small business to receive the award of the contract.<sup>15</sup> If the transaction occurs more than 180 days after the date of an offer, an award can be made, although it will not count as an award to small business for purposes of the agency's small business goals.<sup>16</sup> So, what about the nature of the procurement?

In a recent OHA opinion, *Modern Healthcare Services, JV*,<sup>17</sup> the appellant (Modern Healthcare) claimed that the awardee should not have been eligible for a small business procurement because the awardee had been acquired by a large firm after submission of its initial offer but prior to award and within 180 days of its bid. Modern Healthcare contended that the awardee was required to recertify its size per 13 C.F.R. § 121.404(g) and that such recertification should have resulted in the awardee being deemed ineligible for award.

The SBA Area Office initially determined that the awardee was not required to recertify its size after the acquisition, because the contract at issue was not a MAC, relying on dicta from a previous OHA decision. Before the OHA sustained Modern Healthcare's appeal and remanded the case to the Area Office for a new size determination, the OHA confirmed that the version of SBA's regulation in effect at the time the awardee certified its size in connection with the submission of its initial offer, including price, was the controlling regulation.

Thus, the OHA applied SBA's regulations in effect in 2018, which referred only to the agency's inability to take small business credit for awards made after a recertification as other than small—not the revised regulation that came into effect in late 2020 containing the 180-day limitation on eligibility. Nonetheless, the OHA made an important holding that is likely still applicable under the 2020 version of SBA's regulations: SBA's recertification rules apply to single-award contracts and MACs.<sup>18</sup>

Further still, whether the MAC at issue was set aside for small businesses is also relevant for the analysis.

In *Odyssey Systems Consulting Group, Ltd.*,<sup>19</sup> the GAO had to decide what effect a size recertification made after a merger, sale, or acquisition had on a multiple-award contract that was a set aside for small business. There, Millennium Engineering and Integration, LLC (Millennium), a GSA OASIS 5B IDIQ contract holder, had submitted a proposal for a task order in support of the Space and Missile Systems Center. Thirty-eight days after

submitting its proposal, but before award, Millennium was acquired by another company, causing it to no longer qualify as a small business.<sup>20</sup> The agency then awarded the task order to Millennium. The protester challenged the award before the GAO, arguing that Millennium was ineligible because it was no longer small.

The GAO invited SBA to provide its views on the protest. SBA explained, consistent with the revised regulations, that if a firm recertifies as other than small within 180 days of offer and before award, the firm will generally be ineligible for the award of either a task order or a contract. However, although SBA agreed that Section 121.404(g)(2)(iii) for transactions after an offer but before award applied at the task order level, SBA reasoned that this section was not controlling for the protest at bar.

In SBA's view, Section 121.404(g)(4) "provides an exception to the general rule" for size recertification between offer and award in circumstances involving a MAC set-aside for small businesses. Thus, SBA contended that, pursuant to 13 C.F.R. § 121.404(g)(4), the agency could still make award to Millennium but simply could not receive small business credit for pending and future awards against Millennium's OASIS contract.

While the GAO was "not convinced that SBA's interpretation is the only reasonable interpretation of the regulation," it ultimately deferred to SBA and held that Millennium was properly found to be eligible for award (although GSA could not receive credit toward its small business goals).<sup>21</sup>

### Key Takeaways from *Modern Health Care Services* and *Odyssey Systems*

The takeaway from these decisions is that early planning for a contemplated transaction is critical. A transaction could impact eligibility for a set-aside award depending on (1) the timing and (2) how the opportunity is being procured.

14. 48 C.F.R. § 52.219-28. 15. 13 C.F.R. § 121.404(g)(2)(iii). 16. *Id.*

17. SBA No. SIZ-6114, Nov. 29, 2021. 18. *Id.* at 17-20. 19. B-419731, et al., July 15, 2021, 2021 CPD ¶ 260. 20. *Id.* at 3. 21. *Id.* at 8.

# THE ▶▶ FUTURE OF CORPORATE LAW IS HERE. LEXISNEXIS HAS IT ▶▶ COVERED.

## Related Content

For assistance to filing an agency-level protest by bidders or offerors who believe that the agency has acted erroneously or unreasonably, see

 [BID PROTEST IN GOVERNMENT CONTRACTS \(AGENCY-LEVEL\)](#)

For an overview of filing a bid protest with the U.S. Court of Federal Claims by bidders or offerors who believe that a federal agency has acted erroneously or unreasonably, see

 [BID PROTEST IN GOVERNMENT CONTRACTS \(COURT OF FEDERAL CLAIMS\)](#)

For a discussion related to filing a protest with the Government Accountability Office by bidders or offerors who believe that the procuring agency has acted unreasonably, see

 [BID PROTEST IN GOVERNMENT CONTRACTS \(GAO\)](#)

For guidance to counsel on identifying and obtaining government contracts, see

 [FEDERAL GOVERNMENT CONTRACTS](#)

For a collection of practice notes, templates, clauses, and checklists for federal contractors and their counsel relevant to submitting proposals for and contracting with the federal government, see

 [FEDERAL GOVERNMENT CONTRACTS RESOURCE KIT](#)

For an analysis of common pitfalls for a company to avoid when acquiring a federal government contractor, see

 [COMMON PITFALLS TO AVOID IN THE ACQUISITION OF A FEDERAL GOVERNMENT CONTRACTOR](#)

## Conclusion

Any time a government contractor is considering a potential corporate transaction, it should analyze the potential impact on its current federal awards, pending bids, upcoming competitions and future pipeline opportunities.

The impact will depend on various factors, including the timing of the transaction and nature of the relevant procurements. Early planning and appropriate communication with the government could make a meaningful difference and directly impact the contractor's bottom line. **L**

*Erin M. Estevez is a partner in Holland & Knight LLP's Corporate, M&A, and Securities and Government Contracts practice groups. She advises companies ranging from startups to large, established contractors on regulatory and contractual requirements for doing business with the U.S. government. She can be reached at [erin.estevez@hkllaw.com](mailto:erin.estevez@hkllaw.com).*

*Jeremy D. Burkhart is an associate at Holland & Knight LLP focusing his practice on litigation, government contracting, dispute resolution, and mergers and acquisitions. He can be reached at [jeremy.burkhart@hkllaw.com](mailto:jeremy.burkhart@hkllaw.com).*

*Kelsey M. Hayes is a government contracts associate at Holland & Knight LLP litigating bid protests, claims, and disputes. She can be reached at [kelsey.hayes@hkllaw.com](mailto:kelsey.hayes@hkllaw.com).*

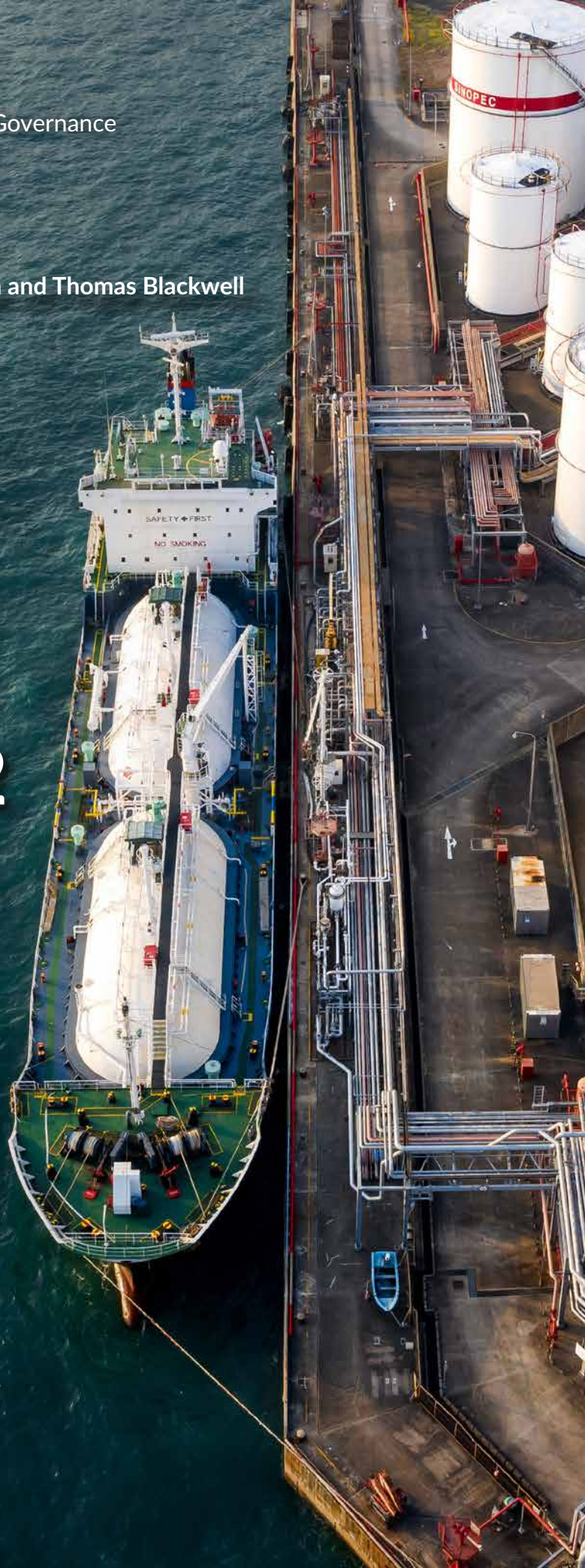
 [RESEARCH PATH: Commercial Transactions > Federal Government Contracting > Articles](#)





Justin F. Hoffman and Thomas Blackwell  
BAKER BOTTS L.L.P.

# Oil and Gas Transactions: Market Trends 2021/Q1 2022



This article discusses market trends in oil and gas transactions from 2021 through the first quarter of 2022, including (1) notable transactions; (2) deal trends with respect to capital markets, mergers, and acquisitions (M&A), and master limited partnerships (MLPs); (3) disclosure trends; (4) legal and regulatory trends; and (5) an outlook for oil and gas transactions going forward.

## Overview

Deal activity increased in 2021 as widely available vaccines allowed for the loosening of travel restrictions and contributed to a rebound in demand, leaving industry professionals relatively optimistic heading into 2022. Production had declined substantially in 2020 following underinvestment in the oil and gas industry that commenced in 2019 and accelerated with the price collapse caused by the COVID-19 pandemic. However, as economic activity returned, production was unable to keep pace with demand as oil prices strengthened throughout 2021. At the same time, upstream oil and gas companies continued to emphasize return of capital and free cash flow generation in response to investor demands for fiscal discipline overgrowth, resulting in nearly flat production growth into 2022. Meanwhile, under pressure from investors focused on the effects of climate change, energy capital investment remained largely focused on investments in the energy transition. M&A in the upstream sector in 2021 was characterized by multibillion-dollar, low-premium consolidations of public companies.

With a backdrop of rising demand and global inflationary pressures, the March 2022 Russian invasion of Ukraine drove global oil prices up to levels not seen since 2008, though prices backed off from those highs in the following weeks. On the natural gas side, the Ukraine situation and Western Europe's reliance on Russian gas are expected to create continued demand for exports of U.S. liquefied natural gas to Western Europe. Despite the rising demand and recent increase in prices, the likelihood of sustained increased U.S. production remains unclear due to numerous factors, including shareholder focus on low leverage, free cash flow and return of capital, permitting and regulatory pressures, and tightness in the services markets, as well as availability and costs of debt and equity capital.

Some of the key federal regulatory changes potentially impacting investment in energy infrastructure in the United States include (1) rollbacks of Trump-era rules that narrowed the application of various provisions of the Clean Water Act; (2) the proposed restoration of several provisions of the National Environmental Policy Act (NEPA) that would grant federal agencies greater discretion in developing project alternatives, restore federal agency discretion to adopt NEPA procedures that are more stringent than the Council on Environmental Quality's regulations, and require agencies to consider direct, indirect, and cumulative effects of major

federal actions; and (3) proposed rules that would rescind Trump-era changes to the Migratory Bird Treaty Act and the Endangered Species Act. More broadly, the Biden Administration rejoined the United States into the Paris Climate Accord and pledged to make the federal government carbon-neutral by 2050.

## Notable Transactions

### M&A

*Coterra's \$17 Billion Acquisition of Cimarex Energy Co.*

On March 24, 2021, Coterra Energy Inc. (formerly known as Cabot Oil and Gas Corporation) and Cimarex Energy Inc. announced an agreement to combine in an all-stock merger of equals transaction valued at roughly \$17 billion. The transaction involved a complementary combination of oil and gas assets across basins and is expected to provide greater stability of free cash flow and return of capital to shareholders. Following closing, Coterra became only the second oil and gas company to announce a variable dividend on top of its regular quarterly dividend, after Pioneer Natural Resources Company did so earlier in 2021. The transaction closed on October 1, 2021.

*Conoco Phillips' \$9.5 Billion Acquisition of Royal Dutch Shell PLC's Permian Assets*

On September 20, 2021, Conoco Phillips announced an agreement to acquire Royal Dutch Shell PLC's Permian assets in a transaction valued at roughly \$9.5 billion. The transaction marked a noteworthy withdrawal of Shell from the Permian Basin and Texas overall, as the company focuses its energy on investment in greener assets. Shell announced that it intended to return most of the proceeds from the sale to shareholders in the form of approximately \$7 billion in share buybacks. The transaction closed on December 1, 2021.

*Pioneer Natural Resources \$6.4 Billion Acquisition of DoublePoint Energy*

On April 1, 2021, Pioneer Natural Resources Company announced it would acquire all outstanding shares of DoublePoint Energy Inc. in a mixed cash and stock transaction valued at approximately \$6.4 billion.

Pioneer issued around 27.2 million of its shares and \$1 billion in cash to DoublePoint's shareholders and assumed roughly \$900 million of DoublePoint's debt and liabilities. The transaction closed on May 4, 2021.



#### *EQT's \$2.9 Billion Acquisition of Alta Upstream and Midstream Assets*

On May 6, 2021, EQT announced it would acquire all the membership interests in Alta Resources Development LLC's upstream and midstream subsidiaries in a mixed cash and stock transaction for \$2.9 billion. EQT gained 300,000 acres in the Marcellus currently producing one Bcf/d of dry gas, along with associated pipeline assets. The acquisition closed July 21, 2021.

#### *Southwestern Energy's \$2.7 Billion Acquisition of Indigo Natural Resources*

On June 2, 2017, Southwestern Energy Company (SWN) announced it would acquire Indigo Natural Resources LLC for \$2.7 billion. The purchase price consisted of cash, stock, and the assumption of \$700 million in liabilities. SWN gained more than 1,000 locations from the acquisition, which closed on December 31, 2021.

#### *Chesapeake's \$2.2 Billion Acquisition of Vine Energy*

On August 11, 2021, Chesapeake Energy Corporation announced it would acquire Vine Energy Inc. in a mixed stock and cash transaction valued at \$2.2 billion. Notably, the acquisition was a zero-premium transaction despite being announced less than

six months after Vine became the only oil and gas company to successfully launch an IPO in 2021. The transaction closed on November 1, 2021.

#### *Chevron's \$1.32 Billion Acquisition of Noble Midstream*

On March 5, 2021, Chevron Corporation announced it would acquire the remaining publicly held shares of Noble Midstream Partners LP in an all-stock transaction valued at \$1.32 billion. The acquisition offered Chevron, which already owned 63% of the outstanding shares of Noble Midstream, access to shale assets in the Permian Basin and natural gas fields in the Mediterranean Sea. The transaction closed on May 11, 2021.

#### *BP's \$723 Million Acquisition of BPMP*

On December 20, 2021, BP p.l.c. announced it would acquire all outstanding public common units of BP Midstream Partners LP in an all-stock transaction valued at \$723 million. The acquisition complemented BP's efforts to become an integrated company by deepening BP's interests in midstream assets that support integration and optimization of its fuels value chain in the United States. The transaction closed on April 5, 2022.

## Deal Trends

### Capital Markets

The traditional public equity capital markets remained challenging for new issuances and are unlikely to be significant sources of funding in 2022 despite the rise in commodity prices, as investors focus more on environmental, social, and governance (ESG) issues and return of capital. Blackstone-backed Vine Energy Inc. went public in March 2021 but was subsequently acquired by Chesapeake Energy Corporation in a mixed stock and cash transaction only a few months later. There remain pockets of potential investments in renewable-based fuel projects that could provide an avenue for some energy capital investment in 2022, including in collaboration with traditional energy companies.

Green bonds, green bond funds such as the PIMCO Climate Bond Fund, and other debt instruments linked to sustainability initiatives are increasingly becoming popular ways for investors to align their portfolios with internationally recognized sustainability goals. Such debt instruments are devoted to financing new and existing projects or activities directly linked to positive environmental impacts such as renewable energy, clean transportation, green buildings, wastewater management, and climate change adaptation. In June 2021, Enbridge Inc. became the first company in the midstream sector to issue green bonds in North America. The bonds, which include a step-up should Enbridge fail to meet its ESG targets, priced at least five basis points below the company's regular debt.<sup>1</sup> While an estimated \$859 billion of green bonds were issued in 2021,<sup>2</sup> the overall market size could eclipse \$1 trillion by the end of 2022 as larger institutions and sovereigns enter the market.

While economic and political uncertainties and increasing ESG concerns are expected to continue to drive market challenges in 2022, opportunities will exist for companies that demonstrate the most sustainable strategies for profitable growth. The drive away from growth-oriented models will continue to enhance investment in service technologies to drive further cost savings. In March 2022, the Securities and Exchange Commission (SEC) proposed a set of rules that would require a wide range of detailed climate-related disclosures for domestic and foreign registrants. For additional information on these proposed rules, see Disclosure Trends below.

Oil prices benefitted from the 2021 rebound, with WTI Crude hitting over \$60 per barrel by March of 2021 and a peak of \$85.15 per barrel in November, ending the year at \$75.21. The price of WTI Crude surged past \$100 per barrel in March of 2022 to a high of \$119 per barrel following the Russian invasion of Ukraine before moderating slightly in the following weeks. The price of crude oil had remained suppressed since 2014, resulting in capital markets activity for most operators shifting away from traditional

IPOs and unsecured debt issuances towards direct investment, hybrid and secured debt offerings, and liability management transactions. Additionally, many operators continue to rely on internally generated cash flows to fund capital expenditures. In lieu of traditional underwritten public or private offerings of equity and unsecured debt, oil and gas issuers have turned to debt exchanges, secured bond deals, private and/or secured convertible note offerings, institutional term loans, and investment by private equity investors to raise capital and manage upcoming maturities.

The high-yield debt markets continue to present difficulties for more speculative energy credits, especially in the new issue market. Depressed interest rates as a result of the Federal Reserve's policy in 2021 have led to low-yield overall in the debt market, making high-yield in the upstream particularly unattractive to investors given the recent default profiles. Most high-yield transactions are being used to refinance existing debt. However, rising interest rates and increased demand for oil and gas in 2022 may drive some additional appetite for energy-related debt in the near term, but uncertainties caused by geopolitical events and concerns about the overall economy's strength have presented material uncertainty in the capital markets due to lack of clarity on which direction commodity prices are headed. Fitch issued a neutral sector rating for North American Oil and Gas in December 2021, reflecting the expectation of continued capital discipline, moderate growth, and focus on free cash flow.

In the bank markets, lenders continued to tighten the terms of reserve-based lending facilities and reduced the borrowing base of some companies by double-digit percentages in what amounted to be a contentious year for redeterminations. Several prominent U.S. banks continue to shy away from fossil fuel projects and have publicly announced their opposition to financing new projects as pressure from activists and institutional investors increased.

### M&A

M&A in the upstream sector in 2021 was characterized by multibillion-dollar, low-premium consolidations of gas-focused public companies. Many legacy oil and gas companies remain focused on opportunities to lower carbon output through divestment and/or acquisition of lower-emissions assets, and emerging reporting and disclosure standards for ESG continue to be a focus.

As discussed above in Notable Transactions, the majority of 2021's marquee deals involved further acreage consolidations in the Permian Basin. These large deals were generally characterized by all-stock consideration, moderate premiums, and competitive geographic and structural synergies. The largest deal, Royal Dutch Shell PLC's sale of its Permian Basin assets to Conoco Phillips, represented nearly double the value of British Petroleum's sale of its Alaska upstream assets in 2020. The trend of consolidation

<sup>1</sup> See JWN Media, *Enbridge Captures 'Greenium' with SLB Debut* (June 25, 2021). <sup>2</sup> See Reuters, *Global Issuance of Sustainable Bonds Hits Record in 2021* (Dec. 23, 2021).

...changes have spurred numerous MLPs to complete simplification transactions... [which] have included, among others, the elimination of the incentive distribution rights in exchange for common units, third-party buyouts, the rollup of the MLP back into the corporate sponsor, and electing to be taxed as a C corporation.

activity—as upstream companies search for scale to protect against prolonged lower commodity prices and continued demand uncertainty—is expected to continue.

### MLPs

Since the 2014 oil price decline, MLPs have not been able to sustain a full recovery and the access to equity capital markets for such issuers has largely dried up. MLPs have also suffered from investors' move to index funds, most of which cannot hold partnership interests. This has led to an increased cost of capital for MLPs and a shift from external equity capital toward more internal financing for growth capital expenditures. MLPs' incentive distribution rights, which represent the sponsor's right to an increasing share of the MLP's distributions as certain distribution targets to the common unitholders are met, have also weighed on the cost of capital for MLPs, especially for MLPs making distributions at the upper end of such targets (known as being in the high splits).

These factors were exacerbated by tax reform that lowered the corporate tax rate in December 2017, and by a Federal Energy Regulatory Commission (FERC) ruling in March 2018 that raised concerns about the ability of some pipeline MLPs to consider unitholder taxes in determining the rates chargeable to certain customers (discussed further in FERC and Pipeline Tariffs under Legal and Regulatory Trends below).

These changes have spurred numerous MLPs to complete simplification transactions. These simplification transactions have included, among others, the elimination of the incentive distribution rights in exchange for common units, third-party buyouts, the rollup of the MLP back into the corporate sponsor, and electing to be taxed as a C corporation.

### Disclosure Trends

#### Hydraulic Fracturing and Climate Change

Environmental and regulatory disclosure has become increasingly important for oil and gas companies. For example, with the heightened focus on hydraulic fracturing and increased earthquake activity in certain areas, issuers' disclosure in the business section

and in the risk factors of their securities offering documents and reports filed with the SEC has become more detailed regarding restraints or potential restraints to operations that could be imposed upon such companies by federal and state governmental bodies.

Climate change has also become a hot-button issue and many oil and gas companies have started to pay close attention to how the risks and opportunities associated with climate change may affect their disclosure. In 2010, the SEC issued interpretive guidance on how climate change may impact an issuer's risk-related disclosures. The SEC's interpretive guidance focused on four areas where climate change may impact such disclosure:

- The impact of developments in legislation and regulation concerning climate change, including greenhouse gas emissions laws and cap and trade systems
- The impact of treaties and national accords relating to climate change
- The indirect risks associated with climate change regulation and business trends with respect to climate change, including changes in consumer demand away from products that result in significant greenhouse gasses, increased demand for alternative sources of energy, and the reputational effects an issuer may face related to the public's perception of its greenhouse gas emissions
- The physical impacts of climate change, including the effects on the severity of weather, the arability of farmland, and the availability and quality of water, and how such effects may affect the issuer's operations and results

In 2021, the SEC responded to increasing investor demand for climate and other ESG information from public companies with its announcement and implementation of an all-agency approach. SEC's ultimate objective is to update the 2010 guidance to account for post-2010 developments and put in place a comprehensive climate-related disclosure framework that will result in disclosures that are consistent, comparable, and reliable. A formal rule proposal on climate-related disclosures was released on March 21, 2022.<sup>3</sup>

The proposed rules mandate a wide range of disclosures, including (1) oversight and governance of climate-related risk; (2) how the company identifies climate-related risks; (3) how those risks have materially impacted or are likely to materially impact its business and financial statements in the short-, medium-, and long-term; (4) how those risks have affected or are likely to affect the company's strategy, business model, and outlook; (5) the company's process for identifying, assessing, and managing the climate-related risks and whether (and how) those processes are integrated into overall risk management systems; and (6) if applicable, information regarding the role of carbon offsets or renewable energy certificates and the use of an internal price on carbon and scenario analysis in a company's climate-related business strategy.

Many companies in the oil and gas sector are affected by climate change legislation, regulation, policies, or impacts and have begun to regularly assess how the foregoing areas impact their business to determine if any climate change-related risk factors or other disclosure are needed. Recently, several major oil and gas companies have begun to follow the recommendations of the Financial Stability Board Task Force on Climate-Related Financial Disclosures (TCFD), with the issuance of more detailed disclosures and reports regarding potential long-term climate change impacts and emissions reduction impacts and analyses. The TCFD recommendations for climate change disclosures focus on governance, strategy, risk management, and metrics and targets used to assess climate-related risks.

#### Proved Undeveloped Reserves (PUDs)

An item that has received a renewed focus by the SEC in recent years is disclosure of PUDs. The SEC has frequently issued comments with respect to an issuer's disclosure of PUDs and

specifically with respect to how such issuer's development plan provides for the required development of PUDs within five years of booking, known as the five-year rule. In a low oil and gas price environment, especially with many oil and gas companies facing liquidity constraints, the five-year rule for booking PUDs often results in a reduction in the amount of PUDs disclosed as companies no longer have the necessary liquidity to drill or it is less economic to drill at the same rate as in higher price environments. Prior to the recovery of oil prices in 2021, the sustained lower price environment had forced some issuers to remove disclosure of PUDs altogether due to significant reductions in their capital spending plan. Recently, however, many producers have tapped their PUDs to take advantage of higher prices, leading to a reduction in PUD inventory.

Another emerging issue, especially in the Permian Basin, that may affect the PUD disclosure of shale companies is the so-called parent-child well problem. Shale producers who initially touted the tighter spacing of wells (e.g., drilling wells in closer proximity to each other) as a method of increasing the overall amount extracted from a reservoir are now finding that new wells drilled closer to older wells generally produce less oil and gas than the older wells and often also interfere with their output. Similarly, producers have touted multiple layers of productive formations that are in some cases turning out to be depleted by production from shallower zones. This has led several shale producers to discuss up-spacing, reducing the number of production zones, and reducing the total number of their drilling locations as the best way to maximize a well's value, even if it means decreasing the overall amount produced. Parent-child well problems have forced some shale producers to write down their PUDs.

<sup>3</sup> See The Enhancement and Standardization of Climate-Related Disclosures for Investors; Release Nos. 33-11042; 34-94478, 2022 SEC LEXIS 730 (March 21, 2022).





## Legal and Regulatory Trends

### Hydraulic Fracturing

When it comes to regulatory trends in the energy industry, no two areas of interest have drawn more attention in recent years than hydraulic fracturing and climate change. The shift to more unconventional drilling techniques continues to create new regulatory and environmental issues as laws adapt to the new drilling environment.

With respect to hydraulic fracturing, the U.S. government and various states and local governments have moved towards regulating, and in some cases restricting, hydraulic fracturing activity. New York, Maryland, Vermont, and Washington have all banned hydraulic fracturing. In November 2018, Coloradoans voted down a ballot initiative that would have banned new oil and gas drilling within 2,500 feet of homes, businesses, and certain green spaces, a move that would have made much of the state off-limits to drilling. Although the 2018 initiative was defeated, similar ballot initiatives have recently been circulated by interested groups for potential consideration in upcoming elections. In April 2019, the Colorado General Assembly changed the mandate of the Colorado Oil and Gas Conservation Commission from fostering oil and gas development to regulating oil and gas development in a reasonable manner

to protect public health and the environment.<sup>4</sup> In response, the Colorado Oil and Gas Conservation Commission modified its rules to address the requirements of the legislation, adopting increased setback requirements, provisions for assessing alternative sites for well pads to minimize environmental impacts, and consideration to cumulative impacts, among other provisions. The new law also allows local governments to impose more restrictive requirements on oil and gas operations than those issued by the state.

Another prominent trend at the state regulatory level has been the movement to require oil and gas companies to publicly disclose the chemicals used in hydraulic fracturing fluids. The majority of oil- and gas-producing states (including Wyoming, Colorado, California, Arkansas, Michigan, Texas, West Virginia, Pennsylvania, and Montana) have passed laws requiring disclosure of the chemicals in these fluids. Additionally, there has been recent focus on a possible connection between hydraulic fracturing-related activities, particularly the underground injection of wastewater into disposal wells, and the increased occurrence of seismic activities. When caused by human activity, such events are called induced seismicity. Some states, such as Oklahoma, have begun to regulate and limit disposal activity as well as hydraulic fracturing in certain areas that are seeing increased seismic activity.

4. 2019 Colo. SB. 181.

### Climate Change

On the issue of climate change, the U.S. Environmental Protection Agency (EPA) has focused in the past on regulating methane emissions in the oil and gas sector. In May 2016, EPA issued new emissions standards that aimed to reduce methane and other emissions from new or modified oil and gas sources, whether through capturing emissions from compressors and pneumatic pumps or through requiring periodic surveys to identify any other fugitive emissions sources. In September 2020, EPA reconsidered and amended aspects of the regulations, including the fugitive emissions requirements. However, in January 2021, President Biden issued an executive order directing EPA to suspend, revise, or rescind the amendments by September 2021 and to consider proposing new regulations to establish comprehensive performance standards and emission guidelines for methane emissions from existing operations in the oil and gas sector by the same date. The EPA released a proposed rule on November 2, 2021, to impose additional restrictions on emissions of methane, or natural gas, from new and existing facilities owned by companies in the production, gathering, processing, transmission, and storage segments of the oil and gas sector.

Additionally, although the SEC has not adopted any new ESG disclosure rules or reporting standards since first providing interpretive guidance on the subject in 2010, it is facing pressure from investors and legislators to do so. In October 2018, institutional investors representing over \$5 trillion in assets petitioned the SEC to require standardized disclosure by public companies of the ESG factors that impact their businesses. In July 2019, the U.S. House of Representatives' Financial Services Committee rejected a bill that would have required climate change risk factor disclosures along with other ESG reporting standards found in Europe. In 2021, acting SEC Chair Lee issued a statement directing the Commission's Division of Corporation Finance to enhance its focus on climate-related disclosure in public company filings, representing the first significant step toward enhanced climate-related disclosure since 2010.

On March 21, 2022, the SEC voted to propose new rules entitled "Enhancement and Standardization of Climate-Related Disclosures for Investors," which would, for the first time, require registrants to include climate-related disclosures in their registration statements and periodic reports. According to the SEC, the proposed rules are designed to increase transparency and accountability around climate-related risks, and would require public disclosure of climate-related risks and their actual or likely material impacts on business, strategy, and outlook; governance of climate-related risks and relevant risk management processes; direct and indirect greenhouse gas emissions, which,

for accelerated and large accelerated filers and with respect to certain emissions, would be subject to assurance; information about climate-related targets, goals, and transition plans, if any; and impacts of climate-related events (e.g., severe weather events and other natural conditions) and transition activities on financial statements. The proposal was subject to a public comment period through May 2022, after which the rule is expected to be finalized before the end of 2022.<sup>5</sup>

Even without formal disclosure requirements, many issuers are beginning to voluntarily provide ESG information. See Disclosure Trends above for further discussion of the areas that the SEC informed companies they should focus on with respect to climate change.



5. See [The Enhancement and Standardization of Climate-Related Disclosures for Investors](#); Release Nos. 33-11042; 34-94478, 2022 SEC LEXIS 730 (March 21, 2022).

## Pipe Opposition

Over the past several years, there has been a growing opposition towards the use of pipelines. While protests over the Dakota Access Pipeline and the Keystone XL Pipeline gained national attention and have become hot-button political issues, the opposition to pipelines has spread beyond environmental activist groups. Calls from activist investors have led several large banks to announce that they would sell off their stakes in loans funding certain controversial pipelines. In February 2020, the Supreme Court heard oral arguments in

U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration issued a final rule that subjects all gas gathering lines . . . to federal oversight and federal minimum safety standards.

*Atlantic Coast Pipeline LLC v. Cowpasture River Preservation Association*<sup>6</sup> concerning the \$8 billion pipeline that, if built, would have transported over a billion cubic feet of gas per day from West Virginia to North Carolina. However, due to the protracted legal conflicts, Dominion Energy and Duke Energy announced the abandonment of the \$8 billion Atlantic Coast Pipeline project in July 2020. President Biden also issued an executive order revoking the permit granted to TC Energy Corporation for the Keystone XL Pipeline. Most recently, the U.S. Court of Appeals for the Fourth Circuit invalidated a permit issued by the Fish and Wildlife Service for the \$6.2 billion Mountain Valley Pipeline, a 300-mile project to link the Marcellus and Utica shale formations to markets in the Mid-Atlantic and Southeast.<sup>7</sup>

New rules were issued and proposed to address safety and environmental issues concerning the midstream industry. On February 17, 2022, the FERC issued a revised policy statement on the certification of the construction of new interstate natural gas transportation facilities. The policy statement sets forth the factors that the FERC considers in determining whether to issue a certificate for new natural gas pipeline facilities. In the revised policy statement, the FERC placed more emphasis on the consideration of impacts on landowner interests and the exercise of eminent domain, upstream and downstream greenhouse gas impacts, and environmental justice issues, as well as how it should assess project need. On the same date, it also issued an interim greenhouse gas policy statement that sets a threshold for emissions that the FERC will consider to be significant and indicated that it would require mitigation of emissions impacts. However, the FERC withdrew both the revised certificate policy statement and the interim greenhouse gas policy statement on March 22, 2022, returning them to draft status, and established a new public comment period. Further developments are expected on the form and substance of the FERC's policies on new and expanded natural gas facilities and greenhouse gas emissions. For safety issues, the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration issued a final rule that subjects all gas gathering lines (even if previously unregulated) to federal oversight and federal minimum safety standards.



To review previous editions of the Practical Guidance Journal, follow [this link to the archive](#).

## Related Content

For a detailed discussion of the unique oil and gas issues for transactional lawyers, see

[OIL AND GAS INDUSTRY GUIDE FOR CAPITAL MARKETS](#)

For a chart that summarizes the U.S. federal securities laws applicable to exchange offers and cash tender offers for debt securities, see

[U.S. SECURITIES LAWS APPLICABLE TO DEBT EXCHANGE OFFERS AND CASH TENDER OFFERS CHART](#)

For guidance on the responsibilities and activities of counsel during the pricing and closing of a municipal bond issue and some of the considerations to be mindful of during this process, see

[MUNICIPAL BOND PRICING AND CLOSING](#)

For information on trends in the private investments in public equity (PIPE) market, see

[MARKET TRENDS 2020/21: PIPES](#)

For an overview of the applicable securities laws and regulations, securities offering process, disclosure and corporate governance obligations, and stock exchange requirements for a securities practitioner working with a private equity firm, see

[PRIVATE EQUITY INDUSTRY GUIDE FOR CAPITAL MARKETS](#)

For an analysis of the impact of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) on private equity funds and managers, see

[DODD-FRANK AND PRIVATE EQUITY: THEN AND NOW](#)

## FERC and Pipeline Tariffs

In March 2018, the FERC announced it would no longer allow MLPs to include an income tax allowance in the rates charged to customers of certain pipelines through cost-of-service tariffs, which are based on an MLP's operating costs and a fixed capital charge. This sent shock waves through the midstream industry as MLPs with a cost-of-service model would no longer be allowed to include an income tax allowance in their operating costs, thus reducing the rates charged to customers. This ruling has no effect on rates charged under negotiated or discounted contracts that differ from the cost-of-service-based tariff.

In July 2018, the FERC provided some relief to MLPs when it clarified that (1) pass-through entities that are not directly subject to income taxation that remove the income tax allowance from their cost-of-service calculation also can completely eliminate accumulated deferred income taxes (ADIT) from this calculation and do not have to return the balance of their ADIT to customers, which is an offsetting benefit to the negative impact of the elimination of the income tax allowance; (2) pass-through entities that are not directly subject to income taxation could be eligible to book a tax allowance in their cost-of-service calculation if their income or

losses are consolidated on the federal income tax return of their corporate parent; and (3) an MLP will not be precluded in a future proceeding from making a claim that it is entitled to an income tax allowance based on a demonstration that its recovery of an income tax allowance does not result in a double-recovery of investors' income tax costs.

The 2018 FERC rulings primarily affected MLPs operating interstate natural gas pipelines under a cost-of-service model. Most gas pipelines, including MLP pipelines, were required to submit a filing to the FERC showing the impact of the elimination of the tax allowance or the reduction in the corporate income tax rate. MLP gas pipelines were also given the option to make a onetime rate reduction that reflected the lower corporate income tax rate, but not the immediate elimination of the income tax allowance. The change in the income tax allowance policy and the corporate income tax reduction will continue to be issues in rate proceedings involving interstate natural gas pipelines, particularly for those pipelines that had rate moratorium agreements in place when the changes first occurred and are required to make filings to set new rates when those agreements expire.

<sup>6</sup> 140 S. Ct. 1837, 207 L. Ed. 2d 186 (2020). <sup>7</sup> *Appalachian Voices v. United States Dept. of Interior*, 2022 U.S. App. LEXIS 3147 (4th Cir. Feb. 3, 2022).

For FERC-regulated MLP oil pipelines, the FERC directed the pipelines to reflect the elimination of the income tax allowance in their page 700 of FERC Form No. 6 reporting and stated that it will incorporate the effects of eliminating the allowance on industry-wide oil pipeline costs. For both gas and oil pipelines, the FERC could require pipelines to revise their rates in individual proceedings (including initial rate filing, investigation, or complaint proceedings) or through other action. These proceedings could also address whether other pass-through entities that are not MLPs are entitled to an income tax allowance.

In 2020, the FERC undertook the five-year review of its oil pipeline rate index and issued an initial order on December 17, 2020, adopting a revised formula for calculating the interstate oil pipeline rate index level. The initial order set the rate index for the five years starting July 1, 2021, as the Producer Price Index for Finished Goods (PPI-FG) plus 0.78%. However, the FERC issued an order on rehearing on January 20, 2022, that revised the formula to PPI-FG minus 0.21%. The lower indexing adjustment resulted from the FERC adjusting the data set used to assess pipeline cost changes from the middle 80% to the middle 50%, taking into account the elimination of the income tax allowance and previously accrued accumulated deferred income tax balances from the FERC Form No. 6 page 700 summary costs of service of MLP-owned pipelines, and using updated page 700 cost data for 2014. The rehearing order

requires pipelines to recalculate their rate ceiling levels using the PPI-FG minus 0.21% formula for the period July 1, 2021, to June 30, 2022. For any rate that exceeds the recalculated ceiling level, the pipeline is required to file a rate reduction with the FERC to be effective March 1, 2022. This will have an industry-wide impact on the degree to which oil pipelines with indexed rates will be able to annually adjust those rates automatically without making a rate case filing at the FERC. The FERC's order on rehearing remains subject to judicial review as several parties have filed appeals in the U.S. Court of Appeals for the Fifth Circuit.

### Reregulation

The trend of deregulation in the oil and gas industry spurred by the Trump Administration has concluded. In 2021, the Biden Administration undertook a series of regulatory actions to review, reconsider, and reverse certain high-profile Trump-era environmental rollbacks. For pipelines, transmission lines, terminals, and other energy infrastructure projects, these reversals posed the risk of longer project timelines and permitting hurdles. Immediately upon taking office in late January 2021, President Biden issued a number of executive orders covering topics from carbon emissions to environmental justice. Those executive orders include a temporary moratorium on new oil and gas leases on federal lands and in the Arctic and the cancellation of the federal permit required to operate the Keystone XL Pipeline. Additionally, President Biden

issued executive orders directing federal agencies to eliminate subsidies for fossil fuels and reversed the Trump Administration's rollback of methane regulations. President Biden has also reentered the United States into the Paris Climate Accord. Last, President Biden has been carefully selecting his SEC appointments, staffing regulators who have made ESG issues a priority, which set the stage for the SEC's formal proposal of mandatory ESG disclosures in March 2022.

The EPA released a proposed rule on November 2, 2021, to impose additional restrictions on emissions of methane, or natural gas, from new and existing facilities owned by companies in the production, gathering, processing, transmission, and storage segments of the oil and gas sector. This is the first time such restrictions would be extended to existing facilities.<sup>8</sup>

Companies across the oil and gas industry should be familiar with the proposed rule and its potential impacts. This proposed rule is not entirely new; the Obama Administration EPA promulgated a New Source Performance Standards (NSPS) rule in 2016 addressing methane emissions from new, modified, and reconstructed facilities in the oil and gas sector, which the Trump Administration EPA rescinded in 2020. This proposed rule reintroduces the 2016 methane NSPS for new facilities and extends it to regulate existing facilities. The EPA held hearings on the proposal in November/December 2021 and sought comments on the proposal, which were due in January 2022. The EPA is currently reviewing those comments.

### Market Outlook

The 2022 outlook for the upstream industry is cautiously optimistic given projected demand increases, despite the continued uncertainty surrounding future governmental restrictions, rig and labor availability, demand, and inflation. Natural gas and liquefied natural gas (LNG) exports are also expected to benefit, particularly for U.S. operators given the tensions in Europe over Russia's actions in Ukraine, although it remains to be seen how the LNG export market will be impacted. Nevertheless, obstacles such as local opposition and litigation, particularly in the midstream sector, will hamper the ability of oil and gas companies to timely respond to these market changes.

The trend of consolidation will likely continue to drive M&A activity, and capital markets access will be driven by robust free cash flow models. Vine Energy Inc., despite launching the only successful oil and gas IPO in 2021, was acquired later that year by Chesapeake Energy Corporation. The outlook for public debt activity is more optimistic, given the effects the anticipated interest rates hikes are expected to have on equity prices, along with the potential for higher commodity prices. If prices remain high enough for long

enough, investor appetite for leverage from upstream players could return, but the industry is also embracing new technologies that will create opportunities for ESG investment and cross-sector deal activity.

On the regulatory and political front, the Biden Administration and the Democratic-led Congress have signaled support for strengthened regulation throughout the industry as the focus on climate change continues to gain momentum. Production levels in the United States are unlikely to reach the 2020 highs of over 13 million barrels of oil per day under the Biden Administration; however, the pressure to replace Russian energy exports to the United States and Europe could change this trajectory and will likely benefit prices going forward.

This article is part of a series of Market Trend articles available on Practical Guidance. Market Trends articles provide insight into regulatory and disclosure trends, recent deal terms and transactions, and projections for the foreseeable future. Market Trends are exclusively authored by practicing attorneys from leading law firms. For more Capital Markets & Corporate Governance market trends, see [Market Trends](#). 

---

*Justin F. Hoffman is a corporate partner at Baker Botts L.L.P. who focuses on delivering practical and strategic advice in high stakes financing transactions and securities law compliance matters. He regularly advises boards of directors, investment banks, and investors on all aspects of public and private capital raising transactions, as well as out-of-court restructurings, Chapter 11 proceedings, and liability management situations. Known for an ability to focus on both fine details and the bigger picture, clients routinely turn to Justin for practical, business-focused solutions to their most complicated problems. He has extensive experience in advising energy companies in connection with securities offerings and acquisition financings, particularly in the upstream, midstream, and oilfield services sectors, as well as coal mining and renewables.*

---

*Thomas Blackwell is an associate at Baker Botts L.L.P. He represents public and private companies in mergers and acquisitions, securities offerings, and general corporate matters. Thomas also advises clients on liability management, acquisition financings, and securities compliance issues, including Exchange Act reporting.*

---

Assistance provided by **Kim Tuthill White, Michael Bresson and Emil Barth**, Baker Botts L.L.P.

---

 **RESEARCH PATH: Capital Markets & Corporate Governance > Trends & Insights > Practice Notes**

<sup>8</sup> See EPA Proposes New Source Performance Standards Updates, Emissions Guidelines to Reduce Methane and Other Harmful Pollution from the Oil and Natural Gas Industry (Nov. 2, 2021).



# Lexis Nexis Offers Support to Ukrainian People during Invasion by Russia

LexisNexis Legal & Professional (LNLP) CEO Mike Walsh recently announced several efforts undertaken by LNLP and the LexisNexis Rule of Law Foundation to support the people of Ukraine in their struggle against invasion by Russia.

ON THE FINANCIAL FRONT, WALSH SAID THAT LNLP has joined other divisions of Reed Elsevier in “supporting aid organizations working across Ukraine to scale up life-saving programs, including trucking safe water to conflict-affected areas, providing health and emergency education supplies as close as possible to communities near the line of contact, providing psychosocial care, and working with municipalities to ensure there is immediate help for children and families in need.”

In addition, Walsh said, a number of the company’s products, solutions, and projects developed and supported by the LexisNexis Rule of Law Foundation “are focused on helping citizens and strengthening legal infrastructures in the Ukraine and around the world.”

- The LexisNexis Rule of Law Monitor continuously tracks public sentiment on the rule of law in 170 countries to create greater worldwide transparency and raise real-time awareness of rule

of law issues. The Monitor has found that 67% of the world population disapproves of the Russian invasion of Ukraine.

- The free eyeWitness to Atrocities App, developed by LexisNexis in partnership with the International Bar Association, allows Ukrainian citizens to document evidence of war crimes using their smartphones.
- The Human RightsApp, developed by LexisNexis and the Australian Human Rights Commission, provides free access to all international human rights law via smartphone.
- Materials used by the Ukraine Advice Project UK, which provides free UK immigration and asylum advice for Ukrainians and their families, are being reviewed for currency and accuracy by Lexis personnel.
- LexisNexis and the LexisNexis Rule of Law Foundation have joined with the International Bar Association, the American Bar Association, and the Union Internationale de Avocats to condemn Russia’s attack on Ukraine.

LNLP has also committed to providing up-the-minute information and practical guidance on legal topics and developments related to the conflict. Law360 is providing free access to War in Ukraine, a compilation of daily news items related to all aspects of the conflict, while Lexis Practical Guidance includes the Ukraine Invasion Resource Kit, covering legal issues emerging from the war.

“We will continue to do everything possible to support our colleagues, the people of Ukraine, and our customers, and our hearts are with all of those impacted by this humanitarian crisis,” Walsh said.

LexisNexis supports the rule of law around the world by:

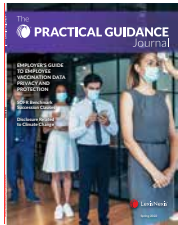
- Providing products and services that enable customers to excel in the practice and business of law and help justice systems, governments, and businesses to function more effectively, efficiently, and transparently
- Documenting local, national, and international laws and making them accessible in print and online to individuals and professionals in the public and private sectors
- Partnering with governments and non-profit organizations to help make justice systems more efficient and transparent and
- Supporting corporate citizenship initiatives that strengthen civil society and the rule of law across the globe.

Additional information about LexisNexis’ activities in support of the rule of law is available at <https://www.lexisnexisrolfoundation.org/>.

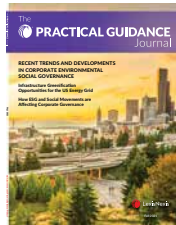


# Practical Guidance Journal Archive

Browse the complete collection of Journals



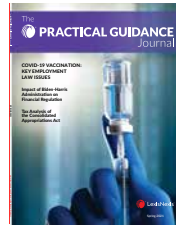
Spring 2022



Fall 2021



Summer 2021



Spring 2021



Fall 2020



Summer 2020  
Covid Response



Special Edition:  
Coronavirus



Spring 2020



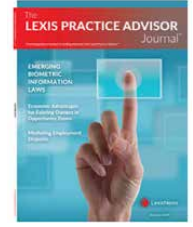
Winter 2019 / 2020



Special Edition:  
Energy & Utilities



Fall 2019



Summer 2019



Special Edition:  
Healthcare Practice



Spring 2019



Winter 2018



Special Edition:  
Civil Litigation



Fall 2018



Summer 2018



Special Edition:  
Labor & Employment



Spring 2018



December 2017



Special Edition:  
Corporate Counsel



Fall 2017



Summer 2017



Spring 2017



Winter 2017



Special Edition:  
Privacy & Data Protection



Fall 2016



Special Edition:  
Finance



Summer 2016



Spring 2016



Winter 2015 / 16





home — office

**Always connected  
legal eBook research  
for wherever your  
work happens.**



Read easily in a web browser or in your preferred eReader.



Search for terms, add notes, highlights and bookmarks for more personalized work productivity.



Link to the Lexis+™ and Lexis® services for deeper online access to law sources.\*

LexisNexis® eBooks

**SHOP FOR LEGAL EBOOKS AT [lexisnexis.com/eReading](https://lexisnexis.com/eReading)  
CALL 800.223.1940**

\*Linking to the Lexis+ or Lexis service may not be available in all titles.  
Access to the Lexis+ or Lexis service requires an active subscription.

LexisNexis, Lexis Advance and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products or services may be trademarks or registered trademarks of their respective companies. © 2021 LexisNexis. OFF04812-00221



Lexis+™



# EXPERIENCE RESULTS.

**A new era  
in legal  
research.**

Superior research, data-driven insights, and practical guidance working all together now to deliver answers faster than ever before.

**Finally, legal research as  
results-driven as you are.**

→ [LexisNexis.com/LexisPlus](https://www.lexisnexis.com/LexisPlus)