LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 32, Number 9 • December 2017

Key Decisions From Delaware Courts

Mergers and Acquisitions

By Francis G.X. Pileggi

A few recent decisions from the Delaware Court of Chancery provide useful information to corporate executives who are involved in the sale or purchase of businesses, or who are involved in joint ventures in which the sales price or the post-closing profit distribution is based on certain milestones being reached and requiring at least one party to use its best efforts, or related standards, in order to reach those milestones that trigger an earn-out.

The cases that follow involve two different but similar standards applicable to the efforts required to reach post-closing milestones in order to trigger payments, and an analysis by the court about whether those standards have been satisfied.

Post-Closing Earn-Out Issues

A Delaware Court of Chancery opinion provides useful insights into the level of effort required to reach certain revenue milestones, for example, in connection with a joint venture or a post-closing earn-out. In *BTG International, Inc. v. Wellstat Therapeutics Corporation*, C.A. No. 12562-VCL (Del. Ch. Sept. 19, 2017), the court

continued on page 10

Labor and Employment Law Changes in the Trump Era

By Matthew B. Schiff and Kathryn C. Nadro

President Trump's first 11 months in office brought significant changes to labor and employment law. The Obama administration succeeded in enacting many pro-employee policies through regulations and executive orders. Due to the largely regulatory nature of those changes, the Trump administration reversed many of those enactments, and has signaled a much more business-friendly stance than its predecessor. Immediate changes to the leadership and agendas for the Department of Labor (DOL), the Equal Employment Opportunity Commission (EEOC) and the National Labor Relations Board (NLRB) have already occurred, along with reversals of policy and positions taken in court.

The DOL

The DOL played a key role in implementing the Obama agenda during the last administration. The Trump DOL has already rolled back many Obama-era regulations, such as ending a narrow reading on requirements for drug testing among applicants for unemployment benefits (*see* http://bit.ly/2nRUlN5); proposing a new rule to end the prohibition on tip pooling between servers and other personnel at restaurants such as bartenders, hosts, and dishwashers (*see* http://bit.ly/2nRUlN5); and proposing a rescinding of the so-called "persuader rule," which required attorneys advising employers facing union campaigns to make mandatory disclosures of their clients (*see* http://bit.ly/295qcWd).

The DOL has also moved to reverse three major administrative interpretations of the Fair Labor Standards Act (FLSA) that had a significant impact on employers: 1) the interpretation regarding which workers are considered independent contractors; 2) which employers are considered "joint employers"; and 3) the overtime rule, which reduced the number of employees exempt from overtime regulations. The DOL has withdrawn a 2015 administrative interpretation that for the first time began with the presumption that a worker is an employee, rather

continued on page 2

In This Issue

Trump Changes

continued from page 1

than an independent contractor. *See* http://bit.ly/2rBbZcf. This interpretation put the burden on companies to show that a worker was not an employee.

Also withdrawn by the DOL was the 2016 administrative interpretation of the definition of "joint employer" under the FLSA. Prior to the Obama-era interpretation, the DOL considered companies joint employers when they had "direct control" over workers, including the power to hire and fire. The withdrawal of these two administrative interpretations is expected to reset the independent contractor and joint employer tests to the standards in place prior to the Obama administration.

Also reversed by the Trump DOL was the Obama-era overtime rule, which raised the salary minimum for classifying workers as exempt from overtime requirements of the FLSA. The Obama regulation never went into effect due to an injunction issued by a Texas federal district court in November 2016. The Trump DOL decided not to continue the Obama DOL's appeal of the injunction, and final judgment was entered against the government by the district judge. The DOL issued a new request for information (RFI) asking for public input to help guide potential new rules. *See* http://bit.ly/2vJUMxi. Public comment on the RFI closed Sept. 25, 2017.

The EEOC

President Trump has appointed new members to the EEOC to fill several vacancies, which will change the majority of the board from Democrat to Republican. The newly composed EEOC is expected to be more "business-friendly" with the appointment of Janet Dhillon as chair. The other new commissioner appointed by President Trump is Republican Daniel Gade, an Iraq war veteran and expert on disability policy. Both Dhillon and Gade have had their confirmation hearings, but as of press time, had not yet been confirmed by the Senate.

The EEOC under Obama issued guidance that Title VII protected against discrimination on the basis of sexual orientation and gender identity. *See* http://bit.ly/1Omlsf1. Dhillon and Gade refused to commit to a position on whether Title VII covers sexual orientation in their recent Senate confirmation hearings. *See* http://read.bi/2yHEnPj.

The Supreme Court is likely to consider whether Title VII protects against discrimination on the basis of sexual orientation, as there is a ripe circuit split on that issue. Current EEOC guidance indicates that Title VII protects against discrimination on the basis of sexual orientation, a viewpoint that the U.S. Court of Appeals for the Seventh Circuit shares as of April 2017. *See* http://bit.ly/2oFN9Vp.

However, in March 2017, the U.S. Court of Appeals for the Eleventh Circuit reached the opposite conclusion, holding that binding precedent prevented it from finding that Title VII protected against sexual orientation discrimination. *See* http://bit.ly/2n5ZQL6. This opinion split can be seen in stark terms in the recent Second Circuit case, *Zarda v. Altitude Express dba Skydive Long Island*, where the EEOC filed an amicus brief arguing that Title VII covers sexual orientation. *See* http://bit.ly/2yHmMqL. In June 2017, however, the Trump DOJ filed a separate amicus brief arguing that Title VII does not cover sexual orientation, and further stating that the EEOC does not speak for the United States on this issue. *See* http://bit.ly/2Aro9H8. At oral argument, the EEOC and the DOJ maintained those opposing positions.

The NLRB

The Trump NLRB is also expected to be more business friendly,

continued on page 6

Matthew B. Schiff is a partner and **Kathryn C. Nadro** is an associate at Sugar Felsenthal Grais & Hammer LLP. Schiff leads the firm's labor and employment group. They can be reached at mschiff@sfgh.com, and knadro@sfgh.com, respectively.

The Corporate Counselor® (ISSN 0888-5877) is published by Law Journal Newsletters, a division of ALM.

The Corporate Counselor P0000-233
Periodicals Postage Pending at Philadelphia, PA
POSTMASTER: Send address changes to:
ALM
120 Broadway, New York, NY 10271

Published Monthly by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, PA 19103
www.ljnonline.com

Ransomware: What To Do When It Happens to You

By Kiran Raj and Mallory Jensen

In an ideal world, your company has all its critical information and data comprehensively and securely backed up, employing strong defenses against hacking, phishing and other cyberattacks. In the event that your company is nonetheless the victim of a ransomware attack, this article provides steps to be taken as part of its response to such an incident. It is meant to be a helpful guide, but the best response generally will depend on different factors, including the scope and severity of the attack, availability of remediation measures, and business sensitivities.

Implement Previously Created Security Incident Response and Business Continuity Plans

Cyber response and business continuity plans should contain the following steps to address a ransomware situation:

1. Conduct an initial analysis of the ransomware. After detecting the ransomware or receiving a ransom demand, it is important to determine, in a timely manner, the original affected device, the scope of infected systems, and any vulnerabilities in the company's systems that were exploited. Conducting such an initial analysis will be immensely helpful during subsequent stages of responding to the ransomware. It is important to carry out this exercise in a forensically sound manner that does not alter or obscure evidence of the attacker's actions.

2. Determine whether the ransomed data, or any parts thereof, exist, and make sure they are properly secured. Assess whether the ransomed, encrypted data exists on unaffected devices, with backup systems, or unaffected servers.

3. Consider what type of data and how much may have been affected or compromised. Knowing whether sensitive information, such as health or financial records, are impacted and how many customers' records may be at issue is important. This information will inform the size of the team that needs to be mobilized in response, as well as the type of response, including breach notification, that may need to be taken.

4. Take steps to prevent continued access by the attacker. It is important to limit the attacker's ability to take advantage of any vulnerability, and to segregate unaffected systems and data.

5. Report internally to the designated individuals to coordinate response. In appropriate cases, it may make sense to apprise senior business leaders, including the Board, who may need to make decisions about how to proceed.

6. Keep contemporaneous records. In consultation with legal counsel, it may make sense to record relevant information about the ransomware attack and your response to it, including logging when the attack was first detected, what steps were taken in response, who was notified, and other important information. To the extent possible, this information should be obtained and recorded in a way that does not delete or modify relevant files.

Hire External Forensic Experts and Legal Counsel As Needed

Depending on the severity of the attack, and the size and capability of your existing IT and cybersecurity teams, it may be necessary to bring in additional help to manage the situation. Many companies specialize in incident response and forensics to supplement your internal team. They can help determine what systems or information were compromised, analyze the available technical information, and identify weak points in the company's systems and processes that should be improved. Outside counsel with experience with ransomware attacks and other security breaches can provide additional legal expertise and leadership, and can help preserve applicable privileges to allow confidentiality for full and frank communication during the ransomware incident and recovery process.

Contact Law Enforcement

This step may already have been completed as part of the incident response plans discussed above, but it is worth noting its importance separately. Even in a widespread ransomware attack where so many companies are affected that even the authorities can seem overwhelmed, it is still important to notify law enforcement. Doing so could help the company if, for example, law enforcement has specific tips or techniques to minimize the damage from the attack. And it helps law enforcement get a full picture of what is happening to different victims of the attack. It also creates a record of steps to address the problem. Of course, law enforcement may not be able to provide immediate help in terms of retrieving data or apprehending the criminals responsible for the attack, but they often can provide other resources and support.

Ideally, the company will have previously established a point of contact with a particular law enforcement agency for this purpose. There should also be consideration to what extent and how the company provides information so as to maintain confidential information and applicable privileges. In-house or outside counsel can help you determine whether and how to notify and work with law enforcement in the wake of a ransomware attack. Throughout the United States, companies can contact local field offices of the FBI and Secret Service, as well

continued on page 4

Kiran Raj is a partner in the Washington, DC, office of O'Melveny & Myers, where he practices in cybersecurity. He was formerly the Department of Homeland Security's highest-ranking attorney focused on cybersecurity and technology. **Mallory Jensen** is an associate in the firm's San Francisco office.

Ransomware

continued from page 3

as the National Cybersecurity and Communications Integration Center, which is part of the Department of Homeland Security; in larger cities, the local police may also have a cybercrime unit.

Check Cyber Insurance Coverage and Notify the Insurer

If your company has cyber or some other type of comprehensive insurance, it may cover a ransomware event and provide coverage for remediation and restoration. The incident response team, in coordination with in-house or outside counsel, should make sure that it understands any requirements set forth in the insurance plan, including notification of the insurer, documentation of the event and damage, or using specific vendors. This may help avoid disputes with the insurance company regarding coverage or claims.

Seek to Restore Data and Return to Business As Usual

Ransomware can stop a company in its tracks by making business-critical data and information unavailable. If that information, including critical documents, has not been properly backed up, the first question asked is how to get the data back. Unfortunately, there are generally only three primary options, none of which is ideal:

1. Hire an expert IT consulting firm or use significant internal resources to attempt to break the encryption. In some cases, it may be possible to find a way to break or otherwise circumvent the ransomware's encryption. However, hackers are using increasingly sophisticated encryption techniques, so the odds of success are low.

2. Work with your IT department or specialists to access data. If you and your customers have ample time and patience, another option may simply be for the company to meticulously attempt to find ways to access the ransomed data. This process may have two parts, though both may not always apply. First, you will want to see if there is any way to restore data, such as through partial backups or by patiently cleaning the system of all the ransomware, perhaps returning it to its state as of an earlier date. Second, to the extent that data is not available to be restored, you will want to seek access to it in some other way, such as through third parties with their own copies of the data, paper copies, or other sources. Unless a complete backup is available, though, these processes will likely not succeed in restoring all data.

3. Understand the full implications and risks of paying the ransom. Giving in to the attackers' demands is rarely a good idea, and should never be done without extensive internal discussion, especially with legal counsel. The Department of Justice (DOJ), including the FBI and other federal agencies, advise against paying the ransom, for various reasons. First, hackers may not provide the encryption key even when the ransom has been paid. Second, the key provided may not work to retrieve the data at all. Third, the key may only work partially, and the hackers will then demand more money before allowing access to the rest of the data. Fourth, paying the ransom also encourages attackers to keep using ransomware and marks the company as a good future target.

However, if no data is backed up, and it is essential to return to normal operations very quickly, companies have made the business-based decision to pay the ransom. The ransom is usually payable only in cryptocurrencies such as Bitcoin, so unless the company has a ready stockpile of such currency, it will need to obtain some for this purpose.

Consider Whether Disclosure of the Ransomware Attack Is Necessary

Depending on the severity of the attack, the type of company and the type of information at issue, in-house or outside counsel can help you determine whether you need to notify customers, the Board, auditors, and/or regulators about the event. Here are a few examples to consider:

Per HHS Guidelines on HIPAA, the presence of ransomware on a covered entity's systems constitutes a security incident and is presumed a breach of Personal Health Information (PHI). HHS guidelines state that when there is ransomware on a system, it is a security incident under the HIPAA Security Rule. A ransomware attack at a covered entity thus triggers HIPAA's mandatory security incident response procedures. And when PHI is encrypted by ransomware, the presumption of a breach means that the covered entity must notify the individuals whose PHI was affected, as well as HHS and the media for larger breaches. A company can only avoid notification if it can show that there is a " … low probability that the PHI has been compromised," after evaluating factors set forth in the HIPAA breach notification rules.

For non-PHI, determine whether the hackers may have accessed or acquired Personal Information (PI) data. Some state data breach notification laws require notice if PI was merely "accessed" by an unauthorized individual, while other laws require notice only if the PI was "acquired" without authorization. Ransomware typically only involves unauthorized encryption of data, not theft, but a ransomware attack nonetheless could be viewed as "access" to the data, though no courts or regulators have yet taken a clear position on whether that would be the case. Depending on the attackers' methods and motives, there could also have been acquisition of PI, so a careful investigation of the incident is vital to determine whether customers must be notified.

Depending on industry and nature of breach, it may be necessary to notify regulators and, in some cases, other companies that may be affected or that provided the data.

Depending on the magnitude of the ransomware's effects on the

continued on page 12

Follow Up on False Claims Act Actions

By Jacqueline C. Wolff and Benjamin J. Wolfert

You are the Senior Vice President and General Counsel at Pharmaceutical Company ABC. For years, you have been responding to multiple subpoenas from the Civil Division of the U.S. Attorney's Office in your District. You have produced hundreds of thousands of documents in response. You have held multiple meetings with Assistant U.S. Attorneys and representatives from the U.S. Department of Health and Human Service's Office of Inspector General (OIG), during which the government has asserted that it is investigating whether ABC has been defrauding the Centers for Medicare and Medicaid Services (CMS).

You have spent a significant amount of ABC's monies paying an outside law firm to conduct an internal investigation to determine whether the federal government's suspicions are warranted, and to gather evidence to disprove any such suspicions. Your attorneys have engaged a consulting firm at ABC's expense to conduct analytics showing that any falsity in any of the claims submitted was due to error. You have signed tolling agreements in order to avoid being hit with a complaint while your outside counsel continues to investigate. And throughout this whole period, you have been wondering whether there is an underlying False Claims Act (FCA) *qui tam* that triggered this investigation and that remains under seal.

Imagine then, after six expensive years of investigation, productions and legal fees, the federal government announces it is electing not to intervene and the *qui tam* is unsealed. Then imagine that upon reviewing the complaint, you realize you have a perfect public disclosure bar defense; that is, you can easily get this *qui tam* complaint dismissed because Congress issued a report containing all these allegations a month before the complaint was filed. You breathe a sigh of relief.

But should you? Probably not, because your journey may not be over. Indeed, state attorneys general may be waiting, hoping to file their own state false claims act cases based on the conduct discovered in the recently unsealed federal *qui tam* complaint. And despite the seemingly endless passage of time, these state actions may still be timely.

This article discusses why that is the case, and what you can do to mitigate against the risk inherent in prolonged exposure. While a 50-state survey is beyond the scope of this article, we identify issues that should be on the forefront of your mind if faced with potential state false claims act liability.

Nullum Tempus Occurrit Regi

The doctrine of *Nullum Tempus Occurrit Regi* — translated as "time does not run against the king" — is a common law doctrine providing that statutes of limitations do not run against the sovereign unless the legislature has expressly provided otherwise. (For a general discussion of the *nullum tempus* doctrine, s*ee, e.g., Block v. N. Dakota ex rel. Bd. of U. and Sch. Lands*, 461 U.S. 273, 294 (1983).)

Many states have abolished this doctrine due to its judicial erosion over the years. These states include Colorado, Florida, Georgia, Minnesota, Missouri, Montana, Nebraska, Nevada, New Jersey, New York, North Dakota, South Carolina, South Dakota, West Virginia and Wisconsin. *See Shootman v. Dept. of Transp.*, 926 P.2d 1200, 1207 (Colo. 1996); Fla. Stat. Ann.§ 95.011; Ga. Code Ann. § 9-3-1 (2013); Minn. Stat. § 541.01; Mo. Rev. Stat. § 516.360; Mt. Code. Ann. § 27-2-103; Neb. Code § 25-218; Gen. Sta. Nev. § 3649; N.J. Stat. Ann. § 2A:14-1.2; N.Y. C.P.L.R. § 201 (*McKinney* 2013); N.D.C.C. § 28-01-023; *State ex. rel. Condon v. City of Columbia*, 528 S.E.2d 408 (2000) (South Carolina); SDCL § 15-2-2 (South Dakota); *State v. Kermit Lumber & Pressure Treating Co.*, 488 S.E.2d 901 (W. Va. 1997); Wis. Stat. Ann. § 893.87 (*West*).

Critically and perhaps surprisingly to many, however, this doctrine is alive and kicking in some form in over 30 states around the country. Some states that recognize the doctrine have limited it to apply only to the state itself, and not municipalities, agencies or other political subdivisions. *See, e.g., State Through Dept. of Highways v. City of Pineville*, 403 So.2d 49, 52-53 (La. 1981) (Louisiana Department of Highways is not considered "the state" for purposes of immunity from statute of limitations); *Mayor and Council of Wilmington v. Dukes*, 52 Del. 318, 328-29 (1960) (*nullum tempus* does not extend to municipalities, or state agencies). In other states, the doctrine only applies to the state when acting in its "public" (not proprietary) function. *See, e.g., District of Columbia Water and Sewer Authority v. Delon Hampton & Associates*, 851 A.2d 410 (D.C. App. 2014) (Water and Sewer Authority has functions that are "proprietary in nature and thus beyond the protection of *nullum tempus*"); *People ex. Rel. Ill. Dept. of Labor v. Tri State Tours, Inc.*, 795 N.E.2d 990, 992-93 (Ill. App. 2003) ("A statute of limitations will not apply to bar a claim by a governmental entity acting in a public capacity[.]"). But *nullum tempus* is still out there, and litigants should take note.

In the states that still recognize *nullum tempus*, the state legislature may override it, leaving the question of whether a particular statute of limitations applies to the state in the hands of the statutory interpretation gods. There is a dearth of case law in state courts addressing this issue in the context of state FCA analogues, which is not surprising given that many of these statutes

continued on page 6

Jacqueline C. Wolff is Co-Chair of both the Corporate Investigations and White Collar Defense and the False Claims Act Practice Groups at Manatt, Phelps & Phillips, LLP. **Benjamin J. Wolfert** was a litigation associate at the firm at the time of this writing.

False Claims

continued from page 5

still are in their nascent stages. This leaves wide open the possibility that state attorneys general may exploit this common law doctrine to argue they are immune from the relevant statute of limitations.

So how big of a risk is this? The short answer is that it remains to be seen, but would-be defendants had better be vigilant and familiar with this doctrine in the states in which they do business. In at least one state (Louisiana), the attorney general has affirmatively taken the position that the state is not bound by the applicable statute of limitations with respect to its false claims statute. Other states may follow suit.

Take Washington State, for example. Washington has attempted to cement its *nullum tempus* doctrine by statute, providing in its code of civil procedure that "there shall be no limitation to actions brought in the name or for the benefit of the state, and no claim of right predicated upon the lapse of time shall ever be asserted against the state[.]" Wash. Rev. Code Ann. § 4.16.160. The Washington Medicaid Fraud False Claims Act provides that all civil actions "may be brought at any time, without limitation after the date on which the violation … is committed." *Id*. § 74.66.100(2).

Texas's Medicaid Fraud and Prevention Act specifies a statute of limitations for *qui tam* relators in the event the State elects not to intervene. But the Statute does not contain an express statute of limitations in the event the attorney general elects to bring its own action. *See* Tex. Hum. Res. Code Ann. §§ 36.052, 36.104. Not surprisingly, Texas still recognizes some form of *nullum tempus*. As one example, in *State of Texas v. Nazari*, 497 S.W.3d 169 (Tex. App. 2006), the state did not hesitate to seek damages from various dental groups for false claims dating back more than 10 years.

Maine, too, has a false claims provision that is silent on the statute of limitations applicable to the state. *See* Me. Rev. Stat. tit. 22 § 15. Query on whether this provision, effective Oct. 9, 2013, overrides Maine's *nullum tempus* doctrine.

The analysis could continue, but there is sufficient evidence that states' attorneys general will attempt to seek remuneration for alleged false claims dating back as far as possible. Would-be defendants, therefore, must be mindful not only of the statute of limitations in state false claims acts where they do business, but also of whether those states are bound by the statutes of limitations.

How to Mitigate Risk In View of Prolonged Exposure

There are several steps to take in order to avoid the pitfalls that could accompany lengthy exposure vis-à-vis state false claims actions:

- ***Document Retention***: Retain relevant documents. False claims exposure may well outlast any regularly scheduled email overwriting; so, even when the DOJ has elected not to intervene and the relator in the federal case has decided not to pursue the case, it may be worth retaining the key documents that can be used to defend your case.
- ***Information Gathering, Organization and Retention***: Interview relevant witnesses (about substantive issues and document location) early and thoroughly, documenting the conversations in order to guard against loss of memory, staff turnover at the client and/or law-firm, and the potential for mergers or layoffs. Discovery is expensive enough. If state governments can bring actions premised on ancient conduct, take steps to avoid reinventing the wheel years after the initial *qui tam* is dismissed.
- ***Create a Procedure for Staff Turnover***: Create procedures at your law firm and/or company to mitigate against the impact of staff turnover, relocations, mergers, layoffs, or any other event that might result in documents or information changing hands or laptops being wiped clean for the new user.
- ***Conduct Damages Analyses Early***: You may not want to wait until being served with a state lawsuit to determine the potential exposure. An early, state-specific damages analysis will accelerate and inform decision-making along the way, including regarding the cost/benefit of early settlement versus litigation.
- ***Be Wary of Driving Up Potential Damages***: If an internal investigation gives credence to the government's investigation, discontinuing or changing ongoing sales practices may not only be the right thing to do, but will also prevent you from driving up damages and being subject to injunctive relief in a later-filed state lawsuit.

—❖—

Trump Changes

continued from page 2

with Trump appointee Peter Robb as General Counsel. Robb is on record as being critical of recent NLRB interpretations of "neutral" policies in employer handbooks as being unlawful and prohibiting concerted activity. Such handbook provisions typically prohibit the use of company email or technology for personal uses. The Obama NLRB struck down many of these policies as violating the Section 7 rights of the employees.

Currently pending before the Supreme Court is *Ernst & Young LLP v. Morris*, which challenges arbitration clauses in individual employment

continued on page 8

Employee Claims In Bankruptcy Pose Significant Liability Exposure

Lessons Learned From In Re FPMI Solutions Inc.

By Shane G. Ramsey and David M. Barnes, Jr.

When a corporation determines to file for Chapter 11 protection, questions concerning the status of existing labor and employment agreements and viability of employee claims immediately arise. Indeed, there are litanies of potential pitfalls for companies that file for bankruptcy without strictly following the requirements of federal or state employment laws.

Perhaps the most-well known among these is the Worker Adjustment and Retraining Notification Act (WARN Act), which mandates that companies pay compensation up to average earnings for no more than 60 days. This compensation is paid to replace earnings lost by prematurely terminated employees. If this liability is triggered within 180 days of the bankruptcy filing, such liability amounts to a first-tier, fourth-priority (wages) claim under section 507(a) of the Bankruptcy Code (*see In re Riker Ins. Indus., Inc.*, and *In re Cargo, Inc.*). If triggered during the post-petition period, such liability is a first-tier, first-priority claim under section 507(a) of the WARN Act (*see In re Hanlin Grp.*).

"Back pay" is also a common remedy under other federal and state employment laws, such as Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, as well as the historic common law remedy for unlawful termination due to unfair labor practices.

But these are not the only federal regulatory laws employers should be aware of when contemplating a bankruptcy filing. As the debtor in *In re FPMI Solutions Inc.*, Case No. 16-12142-KHK (Bankr. E.D. Va.) learned, the McNamara-O'Hara Service Contract Act imposes significant monetary penalties for companies that run afoul of its provisions.

The McNamara-O'Hara Service Contract Act

The McNamara-O'Hara Service Contract Act (SCA) requires contractors and subcontractors performing services on prime contracts in excess of $2,500 to pay service employees in various classes no less than the wage rates and fringe benefits found prevailing in the locality, or the rates (including prospective increases) contained in a predecessor contractor's collective bargaining agreement. The U.S. Department of Labor (DOL) issues wage determinations on a contract-by-contract basis in response to specific requests from contracting agencies. These determinations are incorporated into the contract.

The failure of a contractor to comply with the SCA and the regulations promulgated thereunder may result in liability and debarment from contracting with the government for three years.

In *Vigilantes, Inc. v. Adm'r of Wage and Hour Div., U.S. Dept. of Labor*, 968 F.2d 1412, 1418 (1st Cir. 1992) the decision stated that, "The legislative history of the SCA makes clear that debarment of contractors who violated the SCA should be the norm, not the exception, and only the most compelling of justifications should relieve a violating contractor from that sanction."

Furthermore, in *Karawia v. U.S. Dept. of Labor*, 627 F.Supp.2d 137 (S.D.N.Y. 2009), the precedent was set that the contractor's numerous and repeated violations of SCA amounted to "culpable neglect," an aggravating factor that precluded relief from debarment.

For contracts equal to or less than $2,500, contractors are required to pay the federal minimum wage as provided in Section 6(a)(1) of the Fair Labor Standards Act.

For prime contracts in excess of $100,000, contractors and subcontractors must also, under the provisions of the Contract Work Hours and Safety Standards Act, as amended, pay laborers and mechanics, including guards and watchmen, at least one-and-one-half times their regular rate of pay for all hours worked over 40 in a workweek. The overtime provisions of the Fair Labor Standards Act may also apply to SCA-covered contracts.

In re FPMI Solutions Inc.

A 30-year-old Virginia contractor that provides solutions in human resources, human capital, and learning services for commercial and government clients, both in the United States and internationally, paid back more than $3 million in back wages and benefits to workers to resolve the findings of a U.S. Department of Labor (DOL) investigation. Here's what happened.

FPMI Solutions Inc. (FPMI) filed a case under Chapter 11 of the Bankruptcy Code on June 20, 2016. FPMI's bankruptcy filing was precipitated by Western Alliance Bank, FPMI's largest secured creditor, seizing accounts worth about $860,000 when FPMI failed to repay a loan. FPMI then began defaulting on trade debts and payroll obligations.

Additionally, FPMI violated the prevailing wage and fringe benefits provisions of the SCA, specifically for its failure to pay over $3 million in prevailing wage and health and welfare benefits to its employees working in the Washington, DC, area. The DOL found that FPMI failed to pay employees and contractors during several pay periods between June 2016 and October 2016.

Undeterred by FPMI's Chapter 11 filing, the DOL immediately made an appearance in the bankruptcy

continued on page 8

Shane Ramsey is a partner and vice chair of the Bankruptcy and Financial Restructuring Practice Group at Nelson Mullins Riley & Scarborough, LLP in Nashville, TN. The American Bankruptcy Institute recently recognized him as one of the "Forty Under Forty" bankruptcy professionals. **David Barnes** is an associate in the firm's Washington, DC, office.

Bankruptcy

continued from page 7

case and aggressively pursued its claims, taking actions similar to those traditionally employed by a secured creditor or official committee of creditors. For instance, the DOL played an instrumental part in negotiating with FPMI and Apprio, a tech solutions contractor that ultimately purchased the company, on cash collateral and sale terms, advocating for the payment of salaries and benefits owed as well as retention in employment where possible. Ultimately, Apprio purchased FPMI for $1.7 million in a sale consummated by the court in September 2016. FPMI later moved to voluntarily dismiss the case, which the court granted on June 22, 2017.

Implication of the SCA provided a unique wrinkle to this Chapter 11 proceeding. However, this is not the first instance in which the DOL has enforced the SCA to recover millions in back wages.

In the case of USProtect Corporation, a defunct Maryland company that provided security services for federal buildings across the country, the U.S. Bankruptcy Court for the District of Maryland approved a global settlement allowing DOL to recover close to $8 million in back wages, fringe benefits, and 401(k) plan assets for more than 2,000 security guards. The USProtect Corp. case is actually two jointly administered Chapter 11 filings in the U.S. Bankruptcy Court for the District of Maryland: USProtect Corporation (Case No. 08-13637-TJC) and USProtect Services Corporation (Case No. 08-13638-TJC), with Case No. 08-13637 being the lead case.

Takeaways

The FPMI case should be a useful warning to contractors that fall under the purview of the SCA. The best way to avoid falling into hot water with the DOL is to review all of your contracts to determine whether you are required to follow the SCA. The SCA's statutory requirements are not an option — they are mandatory. Citing the precedent in *A to Z Maint. Corp. v. Dole*, 710 F.Supp. 853, 857 (D.D.C. 1989): "[U]nfamiliarity with the requirements of the SCA may only constitute 'unusual circumstances' once; from then on, a contractor is put on notice that strict compliance with the SCA is required."

WageDeterminationsOnLine.gov (https://www.wdol.gov/) is a helpful website that provides a single location for federal contracting officers to use in obtaining appropriate SCA wage determinations for each official contract action.

Also, be sure to hire experienced professionals to ensure that your company remains in compliance with the SCA. It is imperative that you perform an internal self-audit to ensure your employee compensation and record keeping is current and accurate.

Even if your company is facing financial hardship and is contemplating filing for Chapter 11, it is still important to keep your payroll up-to-date and in full compliance with the SCA. If your company does end up in bankruptcy owing past due wages and other benefits, it is in your best interests to cooperate with the DOL throughout the proceedings.

—❖—

Trump Changes

continued from page 6

agreements as violative of the National Labor Relations Act. These arbitration clauses waive employees' collective action rights. President Obama's Solicitor General had filed, on behalf of the NLRB, a petition for *certiorari* with respect to collective action waivers in employee agreements (this petition was consolidated with *Ernst & Young LLP* and *Epic Systems Corp. v. Lewis*). *See* http://bit.ly/2hlKCR8. The NLRB argued that such waivers violate employees' Section 7 and Section 8(a)(1) rights, and chill collective legal actions.

The DOJ under President Trump has taken the opposite view, and filed an amicus brief arguing that the Federal Arbitration Act is a "super statute" that trumps the provisions of the NLRA, which arguably prohibit such arbitration clauses between employees and employers. *See* http://bit.ly/2hlKCR8. At oral argument, the Solicitor General argued on behalf of the Trump administration that such clauses were permitted, and the NLRB's General Counsel argued the opposite position, leading to the strange sight of the government essentially arguing against itself.

Another expected change under President Trump's NLRB is the end of the "joint employer" rule from the 2015 NLRB *Browning-Ferris* decision, which ended the prior "direct control" standard. *See* http://bit.ly/1LDMtIx. Under that standard, an employer must exercise direct control over the terms and conditions of employment to be considered an "employer." Under *Browning-Ferris*, a company may be considered a joint employer of a worker even if another employer of the worker (such a franchisee or employee leasing company) exercises direct control over the terms and conditions of employment. A bill is currently making its way through the House of Representatives to amend the NLRA to undo the *Browning-Ferris* decision. The Save Local Business Act, H.R. 3441, was in the Rules Committee in the House at press time, and is shortly expected to make its way to the floor. *See* http://bit.ly/2iFNuoX.

Conclusion

As the Trump administration closes out its first year, and many important agency positions remain vacant, there may be many additional changes to labor and employment law in the coming years. Companies should remain attentive to announcements from the Trump administration agencies to glean clues about enforcement priorities and changes in policy. Ultimately, acts of Congress and court decisions will be a check and balance on administration actions.

—❖—

Chancery Approves Incorporation of Reference Condition In Section 220 Litigation

By Brett M. McCartney

Books and records actions are heralded as the "tools at hand" for litigators pursuing shareholder claims against a corporation. In fact, the Delaware Court of Chancery has been critical of litigants who failed to take advantage of a shareholder's right to request the books and records of a corporation prior to commencing litigation against the corporation. *See, e.g., Thermopylae Capital Partners v. Simbol*, 2016 WL 368170, at *17 (Del. Ch. Jan. 29, 2016). And while many shareholders have utilized Section 220's summary proceeding to get a corporation's books and records, Delaware courts have approved certain conditions on the use of those records. As discussed below, the Court of Chancery recently approved a company's proposed incorporation condition, assuring the company that all the documents it produces pursuant to a books and records demand will be incorporated, even if not explicitly referenced, in any subsequent litigation where the plaintiff relies on any of the records produced by the company.

Background

In *The City of Cambridge Retirement System v. Universal Health Services*, the shareholder plaintiff demanded certain books and records of Universal Health Services, Inc. (UHS) to investigate corporate wrongdoing for purposes of a potential derivative action. While UHS contested the scope of the demand, it offered to produce certain documents subject to a confidentiality agreement. UHS's proposed confidentiality agreement included an incorporation-by-reference provision, which stated, "the stockholder agrees that the complaint in any derivative lawsuit that it files relating to, involving or in connection with the Inspection demand or any confidential inspection material, shall be deemed to incorporate by reference the entirety of the brooks and records of which inspection is permitted." The shareholder plaintiff refused, and filed an action seeking to compel the inspection of UHS's books and records.

The Court of Chancery has broad powers to impose "conditions as the court deems appropriate" on the inspection rights of shareholders. In *United Technologies v. Treppel*, Delaware's Supreme Court held that the Court of Chancery has the power to restrict the use of a corporation's books and records in any legal action to a Delaware court. And recently, the Court of Chancery approved an incorporation-by-reference condition in *Elow v. Express Scripts Holding*. The condition permits a corporation to respond to "cherry picked documents" that are taken "out of context" with the entirety of the produced records at its disposal.

This condition resembles the court's approach to ruling on motions to dismiss after plaintiffs have taken expedited discovery in support of an application for preliminary injunction. It also provides a backstop against selective inclusion and out of context quoting of corporate records. "In explaining its current judicial pharmacology, this court has noted the efficacy of an incorporation requirement; it provides the court an alternative to relying solely on the 'strong medicine' of Rule 11 where a plaintiff 'takes a document out of context' and 'insists on an unreasonable inference that the court could not draw if it considered related documents.'"

The Ruling

The plaintiff's argument against the incorporation condition was that it allows corporations to manipulate the universe of documents produced to frustrate the prosecution of meritorious claims. Despite acknowledging the potential for this conduct, the court determined that the benefits of being able to eliminate complaints involving misleading citations to a limited subset of records outweighed the potential for malfeasance by a corporation. The court noted that the plaintiff's argument was not frivolous; however, the court held that the interests of judicial and litigants' economy outweighed the potential detriment faced by the plaintiff.

Analysis

The fallout, if any, from the incorporation-by-reference condition decisions remains unknown. Essentially, plaintiff's counsel now needs to weigh whether the risk of not utilizing a books and records demand prior to filing litigation is less pervasive than the risk that a corporation selectively produces records that, if litigation is commenced, makes the potential for dismissal stronger. Also, shareholders may start bringing Section 220 actions in alternative jurisdictions with hopes of avoiding being saddled with forum and incorporation restrictions. Of course, the pendulum could swing back at corporations should the court find, likely in a case that survives a motion to dismiss, that a corporation failed to produce documents responsive to a Section 220 and sanction such conduct.

While such a ruling hardly seems controversial, it could dissuade corporations from trying to take advantage of a landscape that arguably is tipping in favor of the corporate defendants. In any event, the evolution of books and records litigation continues. Practitioners must be mindful that proposed confidentiality stipulations represent the first figurative battle in a fight to determine where litigation can be brought and what the presiding court may consider.

—❖—

Brett M. McCartney (bmccartney@morrisjames.com) is a partner at Morris James in Wilmington, and a member of its corporate and fiduciary litigation group. He practices primarily in the Delaware Court of Chancery and Delaware Superior Court. This article also appeared in the *Delaware Business Court Insider*, an ALM sibling publication of this newsletter.

Delaware Courts

continued from page 1

applied the contractually defined standard of "diligent efforts" to the promotion of a pharmaceutical product, in a post-trial opinion. This discussion of the contractually defined standard of diligent efforts is at least generally analogous to other Delaware decisions that address the standard of "reasonable best efforts" or "commercially best efforts" or the like, to perform certain tasks or to reach certain goals that trigger payments to a seller. *See* http://bit.ly/2zD8R4W. Due to the relative paucity of cases thoroughly analyzing these types of standards, this case is notable.

Background

This case involved a distribution agreement between two pharmaceutical companies. BTG was the larger company and agreed to promote, distribute and sell a drug called Vistogard, that the smaller Wellstat did not have the resources to promote, distribute and sell. After extensive negotiations, the parties agreed to a contractual definition of "diligent efforts" that BTG was required to employ in order to reach various sales goals for Vistogard. In addition, the parties were required to work together to formulate and finalize a business plan that would describe the details for promoting, distributing and selling Vistogard.

Key Findings

The court found that BTG failed to hire a sufficient number of sales representatives, and failed to devote other resources to sell Vistogard, but instead focused most of its efforts and resources on a completely different product in a different division of the company — with instructions from the CEO to keep the costs flat in relation to Vistogard, and not to increase the resources that were necessary to implement the business plan.

The court found that BTG failed to comply with the contractually defined standard of "diligent efforts," and also breached the agreement by not complying with the business plan that required certain resources, including a sufficient number of sales representatives, to be devoted to the sale of Vistogard.

Legal Analysis

The court provided a useful discussion of the elements of a claim for breach of contract and for awarding damages. The court also took the rare step of shifting fees due to bad faith litigation tactics, and explained its reason for doing so. It recited the familiar elements for breach of contract: 1) the existence of a contract, whether expressed or implied; 2) the breach of an obligation imposed by that contract; and 3) the resultant damage to the plaintiff.

BTG took the aggressive approach of filing a declaratory judgment action seeking a declaration that it had not breached the contract. In response, Wellstat asserted a counterclaim for breach of contract. In sum, the court treated the DJ action as a defensive tactic, which failed, in part because Wellstat did not breach the agreement such that it would have excused a performance of BTG.

This 60-page decision provides extensive detailed factual background, which is necessary to fully appreciate the court's thorough analysis. For purposes of this relatively short overview however, the key points in the analysis are based on the court's finding that BTG failed to devote the necessary resources for Vistogard — and instead prioritized the sale and promotion of other BTG products. In addition to failing to comply with the contractual definition of diligent efforts, BTG also breached the agreement by failing to comply with the business plan that required a minimum amount of resources to be devoted to the sale and promotion of Vistogard.

The court also discussed principles applicable to claims for breach of contract damages. The basic remedy for breach of contract should give the non-breaching party "the benefit of its bargain by putting the party in the position it would have been but for the breach." Expectation damages require the breaching party to compensate for the reasonable expectation of the value of the breached contract. These damages are to be measured "as of the time of the breach."

Although expectation damages should not act as a windfall, the "injured party need not establish the amount of damages with precise certainty when a wrong has been proven and injury established," said the court. "Doubts about the extent of damages are generally resolved against the breaching party." Moreover, the court noted that: "Public policy has led Delaware courts to show a general willingness to make a wrongdoer bear the risk of uncertainty of a damages calculation where the calculation cannot be mathematically proven."

Post-Closing Profit Formula

The Delaware Court of Chancery recently ruled prior to trial on a claim relating to post-closing earn-out payments due in connection with an acquisition. In *GreenStar IH Rep, LLC v. Tutor Perini Corporation*, C.A. No. 12885-VCS (Del. Ch. Oct. 31, 2017), the court found that the terms of the agreement were unambiguous and that the facts alleged were sufficient to enter judgment on three of the eight counts in the complaint that sought damages and declaratory judgments relating to the failure of the buyer to make earn-out payments as required by the merger agreement.

Background

This case involved the sale of GreenStar Services Corporation to Tutor Perini Corporation. The agreement provided for a right to receive post-closing earn-out consideration in the event that certain pre-tax profit milestones were achieved. The motion for judgment on the pleadings that this opinion

continued on page 11

Francis G.X. Pileggi is the member-in-charge of the Wilmington, DE, office of Eckert Seamans Cherin & Mellott, LLC. He summarizes key corporate and commercial decisions of Delaware Courts at www.delawarelitigation.com. Reach him at fpileggi@eckertseamans.com.

Global Mobility Objectives and Immigration

By Dilnaz Saleem

Businesses worldwide are looking to tap into international talent pools, as global expansion is now a critical component to success. Moving individuals to the right roles in new locations, and fast, can provide a company with a significant competitive advantage. However, a company's desire for talent mobility may face hurdles and roadblocks in securing work authorization for their employees as part of an international move. How, then, can companies align their global mobility objectives with rapidly changing immigration rules and regulations?

Centralize the Process

Employers should consider establishing dedicated teams to facilitate the process even if a company outsources its relocation and immigration matters. A decentralized approach, one without any set contacts at either a local or a global level, will lead to an inefficient program, missed opportunities, and a lack of minimum consistencies. Employers must have a formalized policy in which management and human resources are involved in the decision-making process of each foreign hire. A centralized policy also allows the immigration process to be easily measured, both in time and in cost. Dedicate one group to maintain responsibility for the immigration function and to oversee the international movement of employees. This type of centralized model ensures the highest level of consistency, simplifies expat administration, and eliminates redundant processes.

Align Business Objectives With the Realities of Immigration Law

It is imperative that all parties involved in a relocation effort understand that immigration rules are constantly changing and are often restrictive and sometimes discretionary. The granting of a visa, and within a specific timeframe, is not always guaranteed. HR leaders must take the time to set expectations with business leaders and their employees as to whether relocation is possible and to set the timeframe for an expected move. Senior leadership should assess future business needs to ensure talent is timely in place. The pressure to remain competitive may result in companies searching for shortcuts to facilitate quick global transfers; however, the best protection is creating a strong culture of immigration compliance at all costs.

The Power of Communication

Employees should be encouraged to remain in direct and regular contact with HR regarding their move, timeline, and any concerns relating to the immigration process. Employers must communicate the purpose and duration of the international relocation at the outset, and maintain a sufficient connection with all transferring employees even if outside counsel handles their immigration matters. It is necessary that clear communication be established early in the process regarding the length of the assignment, if permanent sponsorship is an option, or if repatriation is required. Larger companies with a high number of mobile employees should consider holding regular town hall sessions to provide critical information to employees and managers.

Relocate Strategically And Think Creatively

Not every relocation requires a long-term move or permanent transfer. Short-term assignees, business travelers, rotation/training programs, and commuter assignments are available options that allow for knowledge transfer and global movement at reduced costs to the employer. Every country has its own policies regarding long-term relocation, extended business trips, and taxation implications, which is why it is vital that employers review all options and assess all obligations prior to any moves. Flexibility is key, and avoiding a cookie-cutter approach allows employees to have a positive relocation experience.

Conclusion

A rapidly increasing international workforce makes it critical that employers provide a dedicated mobility function to their employees, develop appropriate workflows, and create internal policies to deal with the limitations of immigration laws and to ensure that there is no compromise when it comes to compliance. HR, in conjunction with senior managers and executives, should review their internal practices to ensure a high-quality experience for their international employees undergoing relocation.

—❖—

Dilnaz Saleem serves as of counsel at Baker, Donelson, Bearman, Caldwell & Berkowitz, P.C. .

Delaware Courts

continued from page 10

decided related to those parts of the complaint that asserted breach of contract claims for failure to make the earn-out payments in the third, fourth and fifth years after closing.

The court determined that, based on a review of the applicable agreement and the facts alleged in the complaint, the seller was entitled to earn-out payments as a matter of law, based on the clear and unambiguous terms of the agreement. The court also determined that the buyer was not entitled to any offset based on any alleged wrongdoing asserted in the counterclaims. The court rejected claims for fraud based on the failure to plead with the necessary particularity.

The relevant provisions in the merger agreement provided for the calculation of the earn-out payments

continued on page 12

Delaware Courts

continued from page 11

based on pre-tax profit. The agreement defined pre-tax profit as the amount calculated and included in a pre-tax profit report compiled in accordance with GAAP. If the pre-tax profit report was not objected to, then the parties would be bound by it for purposes of calculating the earn-out. If there was an objection to the pre-tax profit report, there was a procedure in the agreement providing for binding arbitration.

Analysis

The court recited basic contract principles, including the truism that when, as in this matter, the language of an agreement is unambiguous, the court is bound by the language within the agreement. The court read the agreement as unambiguously providing for the calculation of the earn-out payments due based on the pre-tax profit reports. When, as in this case, there was no objection to those reports, the parties agreed that those reports would be binding in terms of determining the amount of the earn-out payments that were due.

The court specifically rejected the argument of the buyer that the unambiguous provisions of the agreement regarding the binding nature of the report should be subject to a condition that the report would not be binding if the buyer either failed to properly calculate the pre-tax profit or if the buyer allegedly relied on inaccurate financial statements. The court rejected that argument in part, because it would allow the buyer to unilaterally determine when the pre-tax profit report was not considered binding.

Likewise, in rejecting that argument, the court also rejected the argument that the implied covenant of good faith and fair dealing should allow for an implication that the report would only be binding if it was determined to be accurate.

Implied Covenant of Good Faith and Fair Dealing

The court defined the limitations of the implied covenant of good faith and fair dealing, which will not be used when contract language could have easily been drafted to expressly provide for the allegedly missing terms and when the existing contract speaks directly to the issue in dispute. Stated differently, the covenant exists solely to fulfill the reasonable expectations of the parties, and to avoid arbitrary frustrations of the parties' bargain, but in order for the implied covenant to apply, the obligation asserted and the obligation to be implied must not contradict the purposes reflected in the express language of the contract.

The Holding

In sum, the court found that there were "no gaps to be filled" and that the court would not imply a term that is inconsistent with the intent of the parties as evidenced by the express terms of the agreement. Also notable is the court's rejection of the argument that the existence of 13 affirmative defenses made it premature to grant a motion for judgment on the pleadings. The court reasoned that the "rhythmic incantation of multiple affirmative defenses, each revealed in a single sentence, cannot, alone, defeat an otherwise well-supported motion for judgment on the pleadings."

—❖—

Ransomware

continued from page 4

business, notify external auditors. In worst-case scenarios, the ransomware may so impact your business that it is also necessary to notify the company's external auditors. For instance, if the ransomware shuts down the business for any significant period of time, or if you decide to pay a significant sum of money either to the hackers or to outside advisers to retrieve the data, or if the incident is likely to lead to litigation, the effect on the company's functioning and balance sheet may be such that the auditors must be notified.

Anticipate litigation and regulatory scrutiny. Customers whose data was lost or exposed could file complaints in the days and weeks after learning of the ransomware attack. In addition, state and federal regulators, especially those in areas like health and financial services, are increasingly active enforcing cybersecurity regulations, and have the power to fine or seek injunctions against companies that do not have adequate policies and procedures related to cybersecurity, that make missteps in responding to an attack, or that do not notify customers properly. It is essential to work closely with experienced legal counsel to ensure that you are doing everything possible before, during, and after an attack to comply with laws and regulations and to communicate with customers or regulators in a way that may help to head off litigation or an enforcement action.

Prepare for future attacks. Once a company has been successfully targeted, chances are the same hackers or others will have the company in their sights again before too long. It is essential that you update your company's data privacy protocols and processes and its cybersecurity measures in general, in light of vulnerabilities exposed by the ransomware and uncovered in the incident response process.

—❖—