Inside 2Q2021

ACC Association of Corporate Counsel
BALTIMORE
FOCUS

President's Message

Dan Smith

Happy Summer, ACC Baltimore! I hope everyone is making their way through the heat of the season and beginning to emerge from our very long hibernation, that began in the Spring of last year.

As part of my preparation for this quarter's message, I had the opportunity to review what our esteemed (Past) President, Larry Venturelli, wrote. We were in our first two months of the pandemic. We were just getting used to working and schooling from home. He had the chance to provide a recap of our last in-person event, a Winter Social, sponsored by our then, and continuing, Premiere Sponsor, Jackson Lewis. The Chapter, optimistically, had rescheduled the Golf/Spa from May to August. We had a lot to learn.

We are all pandemic pros now. Experienced in the ways of Zoom calls, social distancing, and working from home.

The Chapter held some outstanding programming, virtually, from our Sponsors, that took a look at our current world of COVID (Nelson Mullins answering our questions about employment and COVID-19 vaccines strategies, and DLA Piper informing us about COVID-19 policies and other employment issues as the pandemic evolves) as well as what the world will look like in the wake of COVID (Perkins Coie discussing preserving Privilege as an in-house counsel, Womble Bond Dickinson addressing doing business with financially challenged companies). If you missed these excellent programs, recordings are available on the Chapter ACC page.

The Chapter also received news that one of our own, Larry Venturelli, was named a 2021 ACC Top 10 30-Something. The article about Larry, who was the Chapter's President last year, can be found here. Congratulations to Larry for this honor!

It is very clear that things are changing. With the initial success of the vaccine roll out, we can start thinking (dreaming?) of getting back to what we had before the pandemic, or at least less of what we are doing now. I hope everyone took the opportunity to respond to the survey the Chapter sent out in April, asking you for how you feel and think about getting back to what we had, even in a modified way. The Board and our Sponsors are eager to get everyone back together again, even if it requires some new protocols – and we needed to hear from you about how you feel about moving ahead and how to do it.

The Board recently held a retreat to discuss the rest of the year and what things are going to look like and, based on your feedback and the ongoing developments, we are cautiously optimistic that we can start getting back together again. In fact, as I write this, the Chapter will be holding its first in-person social, hosted by one of our Premiere Sponsors, Nelson Mullins, at Barcocina. We'll be following the current COVID protocols at that event and encouraging everyone to do what is comfortable for them. In fact, this will be the approach as the Board decided to resume in-person lunches this Fall and hold our annual Golf/Spa event (no Spa this year, but we are looking at alternatives) to be held on September 28th (save the date now!). The Chapter will continue to monitor the current COVID-19 protocols from the CDC and encourage people to do what is comfortable for them.

I remain cautiously optimistic about our Chapter's plans. We will continue to be thoughtful about our approach to events and gatherings. With your help and participation, we can build on the momentum we continued through the Pandemic. I'm looking forward to having the opportunity to see everyone again – to meet and mingle and catch up. I hope to see you, in person, at an event soon.

Positively Legal: The Power of Unfocus

By Caterina Cavallaro, Standards Australia, General Counsel

When we think of excellence and achievement, we often think of being focused and staying on task — following our "to do" lists, timetables, and calendar reminders. However, extensive focus uses a lot of energy and can exhaust our brains. Research shows that the brain operates optimally when it toggles between focus and unfocus, needing both to allow the unconscious brain to make connections and solve problems, "develop resilience, enhance creativity, and make better decisions."

The shortcomings of a focused mind

Richard Davidson, a neuroscientist at the University of Wisconsin, calls focus an essential ability. During sharp focus, he says, key circuitry in the prefrontal cortex gets into a synchronized state with the object of focus, which he calls "phase-locking." For example, if "people are focused on pressing a button each time they hear a certain tone, the electric signals in their prefrontal area fire precisely in sync with the target sound. The better your focus, the stronger the neural lock."

There are benefits to sharp focus, but this focus can be limiting, and we can miss making connections. For example: Sharp focus is like the beam of a flashlight. "While a bright and narrow beam of light cast straight out in front of you is terrifically helpful if that's where you need to be looking," Dr. Srini Pillay writes in his book Tinker Dabble Doodle Try: Unlock the Power of the Unfocused Mind, "what about your peripheral vision and the light you might need to see into the murky middle distance?"

Another example is the well-known invisible gorilla study. Participants were asked to watch a basketball game between a team wearing white and a team wearing black. Participants were told to count how many times the white-shirted team passed the ball to one another. A person in a gorilla suit walked right through the game and most participants, focusing on counting the passes, did not notice the gorilla.

The balance to such sharp focus is "defocused attention," something often identified in highly creative people who have a "wider spotlight that gives them access to more elements." These people then have "greater potential to generate more unusual ideas, as they have a wider array of elements than can be combined with the focus of their attention".

But we don't need to be a creative genius to have a "eureka" moment, generate novel ideas, and solve problems. We can all do it by learning to access our default mode network (DMN), a collection of regions that are active during rest and are usually deactivated during focused tasks.

The default mode network

Pillay thinks access to the brain's DMN, known as the "unfocus network," is just as important as the focus network. The process of "unfocusing" does the following:

- Recharges your brain, reducing amygdala activation and creating calmness;
- Activates the prefrontal cortex and enhances innovation;
- Improves long term memory; and
- Increases activity in the DMN.

There are practical ways to engage the DMN and Pillay suggests first introducing them during periods of the day when the brain would be in a natural slump like right after lunch or in the middle of the day.

Positive constructive daydreaming

Positive constructive daydreaming is a specific type of mind wandering for a short period of time, usually 15 minutes or so, and is characterised by "playful, wishful imagery, and planful creative thought" that serves four adaptive functions: 1. future planning, 2. creative incubation and problem-solving, 3. attentional cycling (when an individual can flexibly switch between various informational streams), and 4. dishabituation (which improves learning since an individual is taking short, recuperative mental breaks from externally demanding tasks).

This type of mind wandering that has been shown to help creativity. "While our minds wander," writes Daniel Goleman in his book Focus: The Hidden Driver of Excellence, "we become better at anything that depends on a flash of insight, from coming up with imaginative wordplay to inventions and original thinking." Positive constructive daydreaming is distinguished from other less productive mind-wandering like negative rumination.

During this time, you should engage in a low-key activity such as knitting,

continued on page 3

continued from page 2

gardening, or going for a walk and let your mind wander to something positive like lying on a yacht or a beach or going for a run through the woods with your dog. This wandering then helps us "wander over to a solution."

In addition, going for a walk on a curved path has been also shown to increase creativity. A 2012 study by Angela K. Leung and colleagues tested three groups, one walked in a rectangle, one sat down, and the last walked freely. The group walking freely outperformed the other two in the mental test they were given.

A five-to-15-minute nap has been shown to give one to three hours of clarity and should be done a few times a week.

Occasionally, if you need it for creativity, try napping for 90 minutes.

Doodling can also increase creativity. It can be done during a conference call as it helps a bored or tired mind to stay awake a little longer. A 40 person study in 2009, found that those who doodled during a 2.5 minute dull and rambling voice mail message recalled 29 percent more details from the message when tested.

Block out time for undemanding tasks and holidays

Block out time for daily breaks you find undemanding like walking or doing crosswords, make time for events to break up the monotony of the week, and ensure you take regular vacations.

Goleman describes a conversation he had with Salesforce CEO Marc Benioff who said, "New ideas won't appear if you don't have permission within yourself." When serving as VP at Oracle, Benioff said he took a month off in Hawaii to relax which, "opened up my career to new ideas, perspectives, and directions." It was during one such holiday that Benioff decided to quit Oracle and start Salesforce.

Actively engaging our DMN can help us to find solutions to unsolved problems, become creative, and enjoy ourselves in the process.

ACC News

ACC Executive Leadership Institute: August 30– September 2 (Chicago, IL)

There are two weeks left to give your top performers an exclusive professional development opportunity. Help them reach the level needed to one day lead your department. Nominate them to attend the 2021 ACC Executive Leadership Institute.

ACC In-house Counsel Certification Program

- 12–22 July
- 12 July – 5 August
- 23 August – 2 September

The *In-house Counsel Certification Program* covers the core competencies identified as critical to an in-house career. This virtual training is a combination of self-paced online modules and live virtual workshops. The workshops will be conducted over a two-week period, four days a week for three hours each day.

Mini MBA for In-house Counsel: June Series

In today's evolving climate, it is more important than ever for in-house lawyers to take on a more strategic role, investing in the company's ability to grow. ACC and the Boston University Questrom School of Business are bringing to you virtually their popular *Mini MBA program*. Master the executive skills needed to ensure that you—and your organization—continue to move forward.

The Global Women in Law & Leadership Virtual Conference and Honors Program: June 21-23

The ACC Foundation would like to honor women in the legal profession! This event, taking place virtually, includes programming focusing on soft skills, innovative leadership, and tangible takeaways to help advance female lawyers in today's busy world. *Reserve your spot today*!

ACC Corporate Counsel University®: June–August

Registration is now open for the *2021 Corporate Counsel University®* (CCU). It will be held in Summer 2021, starting the week of June 14. This comprehensive education program is specifically designed for those new to in-house practice or in-house lawyers with less than five years of experience, as well as those who simply need to sharpen their basic practice skills.

2021 ACC Virtual Annual Meeting: October 19-21

It's here! The 2021 ACC Annual Meeting program is ready and it's jam-packed with valuable substantive and career-focused content you don't want to miss. *Check it out*!

2021 Cybersecurity Summit On Demand

Cybersecurity touches every aspect of consumer and corporate culture, and vulnerabilities present grave financial, legal, and reputational risks. Preventing, preparing for, and responding to data breaches in real time are chief concerns in today's workforce. This *on demand conference programming* will keep you apprised of the latest threats and innovations. The recordings will complement your broad understanding of cybersecurity strategies and principles, enabling you to become a more well-rounded, focused, and effective practitioner.

Wage and Hour Law Updates Spring 2021

By Jed Charner, Jackson Lewis P.C.

Wage and hour laws are technical and often complex. However, compliance with federal, state, and local wage and hour laws is critical. Wage and hour lawsuits have dramatically increased, and the number of collective and class action wage lawsuits has exploded. Defense of class and collective actions often results in substantial defense costs, significant time expenditures, disruption to your company, and exposure to considerable liability.

Under federal law, successful plaintiffs can recover liquidated (double) damages and attorneys' fees. Under state law, including Maryland and a new Virginia law (discussed below), employees sometimes can recover treble (triple) damages. In addition, many wage and hour claims are fully or partially excluded from insurance policies (a careful review of your policy is a wise idea). Non-compliance with wage laws can be very costly.

This article updates developments in federal and Virginia state wage and hour laws, including new laws and interpretations of laws that are more employee-friendly than previously. The updates also serve as a general reminder that employers should review their compensation practices to ensure compliance with federal, state, and local laws.

I. New Virginia Overtime Law Becomes Effective on July 1, 2021

Beginning on July 1, 2021, Virginia employers will be subject to new state overtime wage laws. Previously, Virginia had no state overtime wage law, and Virginia employers were only subject to federal overtime laws. If your company has employees working in Virginia (including employees working from homes in Virginia during COVID-19), they will be subject to the new Virginia Overtime Wage Act, effective July 1, 2021. Although similar to the Fair Labor Standards Act (FLSA), the new Virginia law departs from the FLSA in ways that impose more stringent requirements on employers.

Some key elements of the Virginia law are:

1) Overtime Rate of Pay. Like the FLSA, the Virginia law requires employers to pay one-and-one-half times an employee's regular rate of pay for all hours worked in excess of 40 hours in a workweek.

2) Longer Statute of Limitations. The Virginia law imposes a longer default statute of limitations to file lawsuits than the FLSA. Unlike the FLSA, which applies a default two-year period to bring claims and only allows a three-year period if the employee proves that the wage violations were willful, the Virginia law applies an across-the-board three-year claims period.

3) Liquidated Damages, Treble Damages, and Pre-Judgment Interest. Under both the FLSA and Virginia law, an employee can recover liquidated damages for wage violations, i.e., double the amount of wages that the employer unlawfully failed to pay. However, under the FLSA, an employer can escape paying liquidated damages by showing that it acted in good faith, having a reasonable basis to believe that it complied with the FLSA. Under the Virginia law, in contrast, all overtime wage claims are subject to double damages, and there is no "good faith" defense." In addition, the Virginia law goes further and permits treble (triple) damages for "knowing" violations—meaning that the employer knew that it failed to pay the overtime wages owed and acted in deliberate ignorance or reckless disregard as to whether it was paying all overtime wages. Lastly, the Virginia law penalizes employers with 8% pre-judgment interest per year in addition to liquidated or treble damages. This departs from the FLSA, under which an employee cannot recover pre-judgment interest in addition to liquidated damages.

4) Claims Can Be Brought in State Court. FLSA claims are either filed in federal court or, if filed in state court, can be removed to federal court. Overtime wage claims under the Virginia law, however, can be filed and remain in Virginia state court. Generally, state courts are a more attractive, plaintiff-friendly forum for employees to bring claims. Therefore, in addition to the availability of a longer default claims period and greater damages, employees can bring their claims before more traditionally employee-friendly judges and juries.

5) Different Method to Calculate Overtime Rate for Salaried Employees. For employees paid on a salary or some other regular basis, the Virginia law significantly departs from the FLSA's method to determine the overtime pay rate in a manner that can become expensive for employers. Under the FLSA, one formula is used to determine an employee's regular rate of pay regardless of the method of compensation: all wages for the workweek (including commissions and nondiscretionary bonuses) are divided by the employee's total hours worked in the workweek to arrive at the employee's regular hourly rate. Therefore, to calculate the overtime pay rate of a non-exempt salaried employee, you divide the total pay for the week by the total hours worked to determine the regular hourly rate. The employee must be paid 1.5 times that rate for overtime hours. However, under the FLSA, typically a non-exempt salaried employee is considered to have already been paid within his salary the straight time wages (the "one" of the "one and a half" times calculation) for overtime hours. The employer then only owes an extra "half time" for overtime hours.

The Virginia law departs from this method, calculating a salaried employee's regular hourly rate as "one-fortieth of all wages paid for that workweek." The law appears to presume that a salaried employee's salary is only considered payment for the first 40 work hours in a workweek. This appears to preclude considering the salary as the straight-time wages for the hours in excess of 40. This means that, to calculate overtime wages for salaried and other non-hourly paid

continued on page 5

continued from page 4

employees, an employer must divide the weekly wages by 40, and then pay 1.5 times that amount for all hours in excess of 40. This may result in *significantly* more overtime pay than under the FLSA. The following example illustrates the distinction of Federal versus Virginia law:

Employee is paid $800 a week and worked 50 hours in a workweek.

Federal Overtime Wage Calculation

$800 ÷ 50 hours = $16 per hour regular rate

One half the $14 regular rate = $8 per hour (half time additional overtime pay)

10 overtime hours x $8 per hour = $80 in overtime owed

Virginia Overtime Wage Calculation

$800 ÷ 40 hours = $20.00 per hour regular rate

Time and a half the $20.00 regular rate = $30.00 per hour (1.5 times overtime rate)

10 overtime hours x $30.00 per hour = $300.00 in overtime owed

In this example, the Virginia law mandates 3.75 times more overtime pay than federal law. The impact of this is amplified if a salaried employee prevails in a lawsuit claiming to have been wrongly classified as exempt and therefore is entitled to overtime wages for weeks in which he worked more than 40 hours. The employee would automatically be entitled under Virginia law to double damages even if the employer had a good faith reason to believe it was in compliance. In this case, the employer would pay 7.5 times (3.75 x 2) the overtime wages it would have paid under federal law!

Key Takeaway: If your company has employees working in Virginia, review your overtime pay practices to ensure compliance with the new Virginia state law. Misclassification of employees and failure to properly pay overtime wages to non-exempt salaried employees can have devastating financial consequences.

II. Biden Administration Withdraws or Proposes to Withdraw Trump Administration Employer-Friendly Wage Rules.

The Biden administration's U.S. Department of Labor (DOL) has either withdrawn or proposed to withdraw three employer-friendly Final Rules published during the previous administration. The DOL's walk-backs of the Trump-era Final Rules exhibits the current administration's shift to more employee-leaning wage rules. Two of the three Rules, and the effect of their withdrawals, are discussed below.[1]

A. Independent Contractor Final Rule

On January 7, 2021, in the waning weeks of the Trump administration, DOL published a Final Rule defining the standard to determine whether an individual is an employee or independent contractor. The regulation's intended effective date was March 8, 2021. On March 4, 2021, the Biden DOL delayed the Rule's effective date. On May 5, 2021, the Biden DOL officially withdrew the Rule.[2]

Why Is The Independent Contractor Rule Important?

The FLSA applies only to employees, and not to independent contractors. An employer must pay non-exempt employees the federal and state mandated minimum hourly wages and overtime wages and must maintain a laundry-list of records regarding employees, including exhaustive records regarding their dates of employment, hours worked, and earnings. However, these laws do not apply to workers who are properly classified as independent contractors. The recent expansion of the "gig economy" – a sector of the service industry performing work on a freelance or temporary basis – has pushed to the forefront the issue of when workers properly can be classified as independent contractors.

Historically, What Has Been the Legal Definition of Employee Versus Independent Contractor?

The FLSA itself does not define who constitutes an "employee," other than simply as an individual "employed by an employer." Similarly, prior to the January 2021 Rule, the DOL had never issued a generally applicable regulation distinguishing between an independent contractor and an employee under the FLSA.[3] Instead, courts and the DOL have applied some variation of an "economic reality test," a standard derived from a series of 1940's Supreme Court cases.[4] The test considers the "economic realities" of the relationship between a worker and the putative employer. Courts generally have applied a six-factor test weighing: (1) the degree of control that the putative employer has over the manner in which the work is performed; (2) the worker's opportunities for profit or loss dependent on his managerial skill; (3) the worker's investment in equipment or material, or his employment of other workers; (4) the degree of skill required for the work; (5) the permanence of the working relationship; and (6) the degree to which the services rendered are an integral part of the putative employer's business.[5]

However, the "economic reality" test has not been applied uniformly. Although

continued on page 6

[1]The third Final Rule withdrawn was issued in December 2020 and amended the tipped employees regulations. *See* https://www.dol.gov/agencies/whd/flsa/tips. On April 28, 2021, DOL announced a final rule delaying the effective date of three portions of the 2020 Tip final rule for eight months, until December 31, 2021. *See id*.

[2]*See* https://www.federalregister.gov/documents/2021/05/06/2021-09518/independent-contractor-status-under-the-fair-labor-standards-act-flsa-withdrawal.

[3]DOL has issued regulations applying a multifactor analysis for independent contractor status under the FLSA in certain specific industries. *See, e.g.*, 29 CFR 780.330(b) (applying a six-factor economic reality test to determine whether a sharecropper or tenant is an independent contractor or employee under the Act); 29 CFR 788.16(a) (applying a six-factor economic reality test in forestry and logging operations with no more than eight employees).

[4]*See NLRB v. Hearst Publications, Inc.*, 322 U.S. 111 (1944); *United States v. Silk*, 331 U.S. 704 (1947); *Bartels v. Birmingham*, 332 U.S. 126 (1947); *Rutherford Food Corp. v. McComb*, 331 U.S. 722, 728 (1947).

[5]*See, e.g., Schultz v. Capital Int'l Sec., Inc.*, 460 F.3d 595, 602 (4th Cir. 2006); *Real v. Driscoll Strawberry Assocs., Inc.*, 603 F.2d 748, 754 (9th Cir. 1979). These factors are often called the "Silk factors" in reference to United States v. Silk, 331 U.S. 704 (1947), the Supreme Court case from which they derive.

continued from page 5

the heart of the inquiry is whether "as a matter of economic reality" the worker "is economically dependent on the business to which he renders service or is, as a matter of economic reality, in business for himself,"[6] the application of the test and even the articulation of the factors has varied.[7] This has led to conflicting circuit court decisions regarding the same types of workers.[8] Furthermore, courts have made clear that the analysis should draw from the totality of circumstances, with no single factor being determinative.[9] This has led to a lack of judicial uniformity regarding whether any factors are more significant than others and, if so, which factors are more heavily weighed. Similarly, DOL has issued numerous opinion letters and guidance over the decades, sometimes applying differing articulations of the test.[10] Although there are some clear-cut lines of when a worker must be considered an employee under the FLSA, "gig workers" in particular have presented a greyer area of the law.

The Trump-era Rule was intended to be the first federal regulation offering a clear, uniform standard for all industries to distinguish between an independent contractor versus an employee. It also was aimed at allowing businesses more autonomy to classify gig workers as contractors.

What Was the Final Rule's Standard?

The January 2021 Final Rule introduced a two-step approach to determining whether a worker is a contractor or employee. The following two "core factors" are given primary weight and analyzed first:

(1) the nature and degree of the worker's control over the work; and

(2) the worker's opportunity for profit or loss.

Under the Rule, these two factors are to be most probative of the worker's economic dependence because, "if they both point towards the same classification, whether employee or independent contractor, there is a substantial likelihood that is the individual's accurate classification." However, if these two factors point to different conclusions regarding the worker's status, the other three (less probative) factors can help guide the analysis:

(3) the amount of skill required for the work;

(4) the degree of permanence of the parties' work relationship; and

(5) an analysis of whether the individual's work is "part of an integrated unit of production."

Thus, the test looked at five factors, but placed primary weight on the first two factors, with the other three factors considered only if an analysis of the first two is inconclusive.

What Would Have Been the Practical Effect of the Final Rule?

Many employers believed that the Rule provided more clarity, simplified the economic reality test, and allowed more autonomy to classify certain workers as contractors. The Rule intended to simplify the test by focusing more sharply on the primary factors that determine "who is the boss" in the relationship. The intended regulation further clarified that the control factor (factor 1 above) weighs towards independent contractor status to the extent the worker sets his own schedule, chooses his own projects, and/or has the ability to work for others.

The Rule also articulated other elements of the analysis in an employer-favorable manner. The Rule focused on an employer's actual control over the worker rather than "what may be contractually or theoretically possible" for a purported employer to do. This would help employers rebut plaintiffs who challenge their contractor status by focusing on rights a potential employer could exercise as opposed to actual practice. Many other elements of the Final Rule's analysis and examples tilted towards more autonomy for businesses to treat certain workers as contractors rather than employees.

Which Types of Workers Was the Rule Most Likely To Affect?

The Final Rule was expected to have a particularly large impact on the "gig" economy, which has classified many workers as independent contractors. The gig economy is based on flexible, temporary, or freelance jobs, often involving connecting with clients or customers through an online platform. "Gig workers" include rideshare drivers, food deliverers, freelance writers, and even adjunct or part-time professors. Former Secretary of Labor Eugene Scalia stated that the Rule was driven in part by the passage of laws such as California's AB 5, which requires businesses to classify almost all workers as employees rather than independent contractors.[11] By first focusing exclusively on the two factors of control and opportunity for profit and loss, the test tipped more easily towards some gig workers being contractors.

The effect of the Final Rule's standard can be illustrated with the example of

continued on page 7

[6] *See Schultz*, 460 F.3d at 602 (brackets and citations omitted).
[7] For example, the Second Circuit has analyzed opportunity for profit or loss and investment (the second and third factors listed above) together as one factor. *See, e.g., Brock v. Superior Care, Inc.*, 840 F.2d 1054, 1058 (2d Cir. 1988). The Fifth Circuit has not adopted the sixth factor listed above, which analyzes the integrality of the work, as part of its standard, see, e.g., Usery, 527 F.2d at 1311, but has at times assessed integrality as an additional factor, s*ee, e.g. Hobbs v. Petroplex Pipe & Constr., Inc.*, 946 F.3d 824, 836 (5th Cir. 2020).
[8] *Compare, e.g., Sec'y of Labor v. Lauritzen*, 835 F.2d 1529, 1534-35 (7th Cir. 1987) (applying six-factor economic reality test to hold that pickle pickers were employees under the FLSA), with *Donovan v. Brandel*, 736 F.2d 1114, 1117 (6th Cir. 1984) (applying the same six-factor economic reality test to hold that pickle pickers were not employees under the FLSA).
[9] *See, e.g., Keller v. Miri Microsystems LLC*, 781 F.3d 799, 807 (6th Cir. 2015) ("No one factor is determinative."); *Baker v. Flint Eng'g & Const. Co.*, 137 F.3d 1436, 1440 (10th Cir. 1998) ("None of the factors alone is dispositive; instead, the court must employ a totality-of-the-circumstances approach.").
[10] *Compare, e.g.*, WHD Fact Sheet #13, "Employment Relationship under the Fair Labor Standards Act (FLSA)" (Jul. 2008) (applying seven-factor test) with WHD Opinion Letter FLSA2019-6 (applying six-factor test).
[11] Following the passage of the California law, ridesharing companies funded a successful ballot initiative, Proposition 22, to exempt ridesharing and delivery companies from AB 5's requirements.

continued from page 6

a driver for a ridesharing company. Application of the historical six-factor economic reality test, under which no factor is given primacy, lends more easily to concluding that the driver is an employee. Rideshare driving does not require particular skill, the driver does not employ others, some individuals may drive for the same company for years, and the driving services are the crux of the company's business. These factors would weigh towards an employer-employee relationship. Under the new Rule, however, the first step of the analysis considers only two factors: (1) the nature and degree of the worker's control over the work, and (2) the worker's opportunity for profit or loss. A rideshare driver sets his own schedule, determines where and when he wants to work, how far and in which areas he will drive customers, and his opportunity for profit or loss is dependent on those decisions. The analysis likely would not reach the second stage under which additional factors would be considered. Under the Final Rule, such workers often would be contractors and not employees.

The DOL Has Withdrawn the Rule. Now What?

In its May 5, 2021 withdrawal of the Final Rule, the DOL noted that no court or the DOL has ever applied the "core factor"/secondary factor analysis set forth in the Final Rule and, "after careful consideration of the comments received, the Department believes that elevating two factors of the multifactor economic realities analysis above all others is in conflict with the [FLSA], congressional intent, and longstanding judicial precedent." The DOL now "believes that the Rule is inconsistent with the FLSA's text and purpose, and would have a confusing and disruptive effect on workers and businesses alike due to its departure from longstanding judicial precedent." The DOL made clear that it is not currently proposing any new guidance to replace the Trump-era Final Rule. Rather, DOL merely withdrew the Rule and instead left in place "the current economic realities test which allows for determinations that some workers are independent contractors."

Key Takeaway: Although the Trump-era Final Rule would have allowed employers more autonomy to classify workers as contractors, the current DOL withdrew the Rule. Employers should continue to follow the "economic reality" test as applied by courts in their jurisdiction and/or DOL guidance applicable to their industry, recognizing that the current administration has shifted to more employee-friendly rules and enforcement. Employers should consider the shift in approach as part of their risk analysis. Additionally, especially in situations where analysis of different "economic reality" factors conflicts, it may be wise to consult with counsel experienced in advising on such issues.

B. The Joint Employer Final Rule

Near the end of the previous administration, the DOL also issued a Joint Employer Final Rule, addressing the standard for determining whether an employee may be deemed to be jointly employed by two or more employers. This Final Rule established a more employer-friendly standard, abandoning other interpretations that subjected employers to greater risk of liability as joint employers if they were "not completely disassociated" from a worker.[12]

Why Is The Joint Employer Rule Important?

There is a variety of circumstances in which two or more businesses may be considered to jointly employ an individual under the FLSA. In "vertical joint employment" one employer, known as a direct employer, provides workers to a secondary business. The direct employer hires and pays the worker, whereas the secondary business simultaneously benefits from the employee's services. Typical examples of this are businesses that use staffing agency employees, general contractors that use subcontractors' employees, and franchise operators whose operations benefit the franchise (e.g., restaurant franchisees). In these examples, the staffing agency, subcontractor, and franchise operator directly employ workers. However, in many scenarios, courts and the DOL have concluded that the company using staffing employees, general contractor using subcontractors' employees, and franchise owners are joint employers and are liable for wage and hour violations of the direct employer.[13]

Where joint employer status exists, both employers are jointly and severally liable for the other employer's violations of wage laws with respect to those employees. This risk places on companies the responsibility to vet the wage practices of staffing agencies, subcontractors, and franchise operators with whom business is conducted to ensure compliance with the FLSA.

Historically, What Has Been the Joint Employer Test?

The answer is complicated. Different federal circuit courts use different tests,[14] and the test has varied even within individual circuits.[15] In 2018, the Supreme Court

continued on page 8

[12] *See* 23 FR 5905 (Aug. 5, 1958) and former 29 CFR 791.2(a).

[13] In "horizontal joint employment," the other type of joint employment, the employee works for multiple related or associated employers, working some hours for one employer and other hours for the other employer. One example offered by DOL is an employee who works at two restaurant locations of the same franchise, each owned and operated by different legal entities. However, one person is the majority owner of both entities. Managers at each restaurant share the employee between the locations and jointly coordinate the employee's schedule. The employers use the same payroll processor and share supervisory authority. In this scenario, both entities are joint employers. See 29 CFR 791.2(g).

[14] *Compare, e.g., Bonnette v. California Health & Welfare Agency*, 704 F.2d 1465 (9th Cir. 1983) (establishing a four-factor test); *Salinas v. Commercial Interiors, Inc.*, 848 F.3d 125 (4th Cir. 2017) (creating a six factor test); *Layton v. DHL Express (USA), Inc.*, 686 F.3d 1172, 1176-77 (11th Cir. 2012) (identifying an eight factor test); *Zheng v. Liberty Apparel Co.*, 355 F.3d 61, 70 (2nd Cir. 2003) (using a ten factor test).

[15] *See, e.g., Dalton v. Omnicare, Inc.*, 138 F.Supp.3d 709, 717 (N.D. W. Va. 2015) (applying a four-factor test derived from the Ninth Circuit); *Jennings v. Rapid Response Delivery, Inc.*, Civil No. WDQ-11-0092, 2011 WL 2470483, at *3-4 (D. Md. June 16, 2011) (applying a nine-factor test derived from the Second and Ninth Circuits); *Heath v. Perdue Farms, Inc.*, 87 F.Supp.2d 452, 457 n.4 (D. Md. 2000) (applying a nine-factor test derived from the Migrant Workers Act regulations and case law).

continued from page 7

declined to address the issue.[16] The current standard of the Fourth Circuit Court of Appeals (applicable in Maryland, North Carolina, South Carolina, Virginia, and West Virginia) is an employee-friendly standard that deems entities as joint employers when they are "not completely disassociated" with respect to a worker's employment.[17] Joint employment exists when two or more persons or entities share, agree to allocate responsibility for, or otherwise codetermine the essential terms and conditions of a worker's employment.[18] To answer whether both employers indeed codetermine the conditions of a worker's employment, courts in the Fourth Circuit consider six, non-exhaustive factors: (1) Whether the putative joint employers jointly determine, share, or allocate the power to direct, control, or supervise the worker directly or indirectly; (2) Whether the putative joint employers jointly determine, share, or allocate the power to hire or fire the worker or modify the terms of employment; (3) The degree of permanency and duration of the relationship between the putative joint employers; (4) Whether, through shared management or a direct or indirect ownership interest, one putative joint employer controls the other putative joint employer; (5) Whether the work is performed on a premises owned or controlled by one or more of the putative joint employers; and (6) Whether the putative joint employers jointly allocate responsibility over typical employer functions such as payroll, workers' compensation insurance, payroll taxes, or providing facilities, equipment, tools, or materials to complete the work.[19] The Fourth Circuit held that the totality of circumstances is considered and did not place primary emphasis on any of the factors.

What Was the Final Rule's Joint Employer Standard?

The Joint Employer Final Rule established a simpler, uniform, and more employer-friendly standard for "vertical joint employment" scenarios that made it easier for potential secondary employers to avoid joint employer status. The DOL adopted a four-factor test assessing whether the purported joint employer[20]:

- Hires or fires the employee;
- Supervises and controls the employee's work schedules or conditions of employment;
- Determines the employee's rate and method of payment; and
- Maintains the employee's employment records.

Significantly, the Final Rule stressed that actual, not theoretical, exercise of control over the worker, via one or more of the four factors is required to be a joint employer. A company's ability or right to act in relation to the employee does not demonstrate joint employer status without actual exercise of control. The Rule further clarified that an employee's "economic dependence" on a potential joint employer is not relevant to determine whether it is a joint employer under the FLSA. This means that even if the worker is economically dependent on the potential joint employer, *e.g.*, the worker performs a specialty job for which it relies on the potential joint employer, that is not a relevant factor.

What Was The Practical Effect of the Joint Employer Rule?

The Rule made it easier for businesses using the services of another company's employees to escape liability for wage violations. In particular, the Rule's emphasis on actual exercise of control over the worker versus a theoretical right to exercise control made it easier for secondary businesses to avoid joint employer status. As an illustrative example, say that a large department store chain contracts with a janitorial company, which provides cleaning services at the stores. The janitorial company hires and pays its workers and sets the employees' rate and method of pay. The janitorial company has only one client, the large department store chain, and the janitors are economically dependent on the stores. The written agreement between the companies provides that the stores retain the right to: (1) instruct janitors where and how to clean, (2) set the janitors' work schedules, (3) insist that janitors are paid appropriate and legal wages, and (4) decide that a janitor cannot work at any of its stores, which in effect would mean that the janitor is fired. In practice, however, the store chain rarely inserts itself into any of those decisions. Janitors clean the facilities at night after closing when no store managers are present to instruct them. The store is unaware of the janitors' wages and only once in five years has stated that a janitor can no longer work at its facilities. It turns out that the janitorial company has failed to pay overtime wages to its employees, who work between 50-60 hours a week. A group of janitors files a collective action lawsuit against both companies claiming overtime wages. Is the department store liable? Whereas other versions of the joint employer test would place weight on the agreement between the companies that gave theoretical rights of control to the store chain, the Final Rule established a standard looked only at *actual* control. In this case, under the Final Rule, the store did not exercise control over the workers and is not their joint employer.

What Is the Status of the Rule?

The Rule first suffered a blow on September 8, 2020, when a U.S. District Court judge struck it down, finding its terms arbitrary and capricious and in conflict with the FLSA.[21] The DOL appealed that ruling, which remains pending with Second Circuit Court of Appeals. Then, on

continued on page 9

[16] *See DirecTV, LLC v. Hall*, 138 S. Ct. 635 (2018) (denying petition for certiorari).
[17] *See Salinas v. Commercial Interiors, Inc.*, 848 F.3d 125 (4th Cir. 2017).
[18] *Id.* at 141.
[19] *Id.* at 141-42.
[20] The test was from a decision of the Ninth Circuit Court of Appeals. *See Bonnette v. California Health & Welfare Agency*, 704 F.2d 1465 (9th Cir. 1983).
[21] *See State of New York et al. v. Eugene Scalia et al.*, No. 1:20-cv-01689 (S.D.N.Y. Sept. 8, 2020).

continued from page 8

March 12, 2021, the DOL issued a notice proposing to rescind the Joint Employer Rule.[22] The proposal was open for public comment until April 12, 2021.

Now What?

Until formally withdrawn, the Final Rule remains in effect, allowing more flexibility for companies using staffing employees and similar arrangements to more easily avoid joint employer status. However, as with the independent contractor issue, the Rule has little chance to survive. It remains to be seen what standard the current DOL will implement or whether it will simply drop the issue, and the law will remain as interpreted in differing ways by the courts in various jurisdictions.

Key Takeaway: The current administration has shifted to more expansive wage protections for workers, including a more expansive definition of joint employment than under the Trump-era regulations. A finding of joint employment will become more likely. When contracting with a staffing agency or subcontractor to supply workers for your company, carefully vet whether the firm complies with all wage and hour laws to avoid potential joint employer liability.

4844-2326-9095, v. 6

Author:

Jed Charner

Jed Charner is a senior associate in the Baltimore, Maryland office of Jackson Lewis P.C. Jed represents management in all aspects of labor and employment law, with a focus on defending employers in wage and hour litigation, both single plaintiff and collective/class action cases. Jed also advises employers on compliance with federal, state, and local wage laws.

[22] *See* https://www.federalregister.gov/documents/2021/03/12/2021-04867/rescission-of-joint-employer-status-under-the-fair-labor-standards-act-Rule.

Best Practices for Managing Cyber Risks in a Cyber World

By Tara Cho, CIPP/US, CIPP/E, Womble Bond Dickinson LLP

(This paper is based on a Cybersecurity Panel discussion with Tara Cho; David Coher, Principal, Strategic Planning & Power Supply, Southern California Edison; Stephanie Lambert, AVP, Chief Compliance Counsel, NETSCOUT; JoAnna McFadden, Deputy Chief, Assistant US Attorney, Criminal Division; and moderated by Mark Henriques)

One remarkable aspect of the COVID-19 pandemic has been how quickly and completely global businesses were able to pivot to a virtual work environment. Across the world, employees fired up their laptops and got back to work from their living rooms and kitchen tables.

While this can-do spirit helped keep the global economy treading water during 2020, it also led to unprecedented threats to cybersecurity. Each work-from-home employee represents a potential entry point for cyber threats. Given how rapidly businesses had to transition during the pandemic, they also had limited (if any) time for standard diligence or testing prior to deployment.

A number of other factors working against cybersecurity efforts during the pandemic have collided to create more opportunity and ideal circumstances for attackers. Such factors include the need to engage vendors and technology developers that may be operating outside of their normal industries or offerings, limited employee familiarity (or comfort-level) with the technology, and employee job insecurity which may lead risky IT workarounds in the home environment to simply get the work done. Employers found they no longer had complete control over the work environment—a necessary adaptation, but one that brought increased risks.

Also, most companies understandably had to focus on simply maintaining their operations during the pandemic-induced economic crisis. Cybersecurity was not necessarily at the top of the priority list, and in some cases, IT and security personnel may have been among those furloughed due to the pandemic.

Needless to say, the shift to remote working has led to a dramatic increase in exposure. According to the Cost of a Data Breach Report 2020, an annual report produced by the Ponemon Institute and IBM Security, 70 percent of organizations surveyed said remote work would increase the cost of a data breach and 76 percent said it "would increase the time to identify and contain a potential data breach." Having a remote workforce was found to increase the average total cost of a data breach of $3.86 million by nearly $137,000 for an adjusted average total cost of $4 million.

The Internet Crime Complaint Center (IC3) tracked and reported a massive spike in hackers attempting to capitalize on the COVID-19 crisis. In April 2020, online crimes reported to IC3 had roughly quadrupled since January to 4,000 incidents daily, according to Tonya Ugoretz, the deputy assistant director of the FBI's Cyber Division. COVID-19 threat reports alone now account for five times that figure, more than the IC3 saw for all threats in 2019, including unrelated scams, phishing and fraud schemes.

Without a doubt, the pandemic created fertile ground for bad actors. For the first time in history, NETSCOUT observed more than 10 million denial of service attacks in 2020. That's 1.6 million more than the prior year and May 2020 was the single largest number of monthly attacks that NETSCOUT has ever recorded.

continued on page 10

continued from page 9

2020 At Its Worst—Top Cyberattacks

With all of those factors working against companies hoping to protect sensitive information, it is no surprise that 2020 saw a number of noteworthy cyberattacks (although some attacks began even prior to the pandemic). The following are some of the most prominent examples:

- Marriott International: Hackers used compromised credentials from a franchised property. The attack affected personal information of approximately 5.2 million guests. Hotels are targeted not just to obtain and sell personal data but also to compile and sell intelligence related to the location of government officials with security clearances and to track business leaders for high-profile companies.
- Twitter: The popular social media site was hit by a social engineering/phone spear phishing attack to obtain access to Twitter employees' credentials to access internal support tools and tweet from the targeted accounts. High-profile victims of the attack included well-known personalities (Kanye West, Bill Gates, Elon Musk, Jeff Bezos, Warren Buffet, etc.), politicians (Barack Obama, Joe Biden, Mike Bloomberg, etc.) and companies (Uber, etc.)
- MGM Resorts: Information pertaining to approximately 10.6M guests was shared on a hacking forum, again with a focus on high-profile persons, including celebrities, senior executives, employees of major companies, reporters, government leaders and FBI agents.
- Zoom: 500,000 user accounts were posted for sale on the dark web as a result of a credential stuffing attack and easy-to-guess pass codes.
- Magellan Health: A social engineering phishing attack resulted in an exported data and ransomware attack affecting 360,000 patients.
- Finastra: As a software provider to financial institutions including 90 of the top 100 banks globally, Finastra maintains sensitive financial data and was subject to a ransomware attack that disconnected servers (by exploiting vulnerabilities associated with outdated security patches).
- SolarWinds: Nation-state attackers added malware into SolarWinds' Orion software system and the malware was then distributed across SolarWinds customers via regular software updates, impacting numerous federal agencies, Fortune 500 companies and other customers.

The Particular Dangers of Ransomware Attacks

Ransomware predates the COVID-19 pandemic. But the work-from-home environment certainly provided increased opportunities for such attacks, and ransomware attacks bring with them particular risks that should be examined independently of other cyber-attacks.

Ransomware is a type of malware—a malicious software unknowingly downloaded by the user. Often, ransomware is spread through email phishing or by visiting an infected website. Once the ransomware is downloaded, it locks the user out of the computer system until a ransom is paid, typically in Bitcoin or some other form of untraceable cryptocurrency. The (usually anonymous) hacker may even threaten to release sensitive or confidential information if the ransom is not paid.

According to one report, the United States saw a 139 percent increase in ransomware attacks in Q3 2020 alone, with the nation recording 145.2 million ransomware attacks in that three-month span.

As Stephanie Lambert of NETSCOUT notes, paying ransomware hackers could put the victim at risk of Office of Foreign Assets Control (OFAC) actions. OFAC administers and enforces U.S. trade sanctions against targeted countries and groups. Since the victim often does not know the identity of the hacker, there is no way to confirm they are not listed on the sanction list.

What's at Stake?

The costs of data breaches are high—and getting steeper. The average cost of a data breach in 2020 was $3.86 million, as previously mentioned. The United States had the highest average costs in the world, and by sector, breaches are most expensive in the healthcare sector and records with healthcare data hold the highest street value, even over financial or payment data.

Malicious attacks accounted for 52 percent of data breaches in 2020, according to the aforementioned Ponemon/IBM report. System glitches accounted for 25 percent of breaches, while 23 percent could be traced to human error. The report also found that nation-state actors created the most expensive breaches (as compared to financially motivated actors).

The Ponemon/IBM report identified the following breakout of root causes for data breaches:

- Cloud misconfiguration—19 percent;
- Compromised credentials—19 percent;
- Vulnerability to third-party software—16 percent;
- Phishing—14 percent;
- Physical security compromise—10 percent;
- Malicious insider—7 percent;
- Other misconfiguration or system error—6 percent;
- Business email compromise—5 percent;
- Social engineering—3 percent;
- Other—1 percent.

Data records containing customer personally identifiable information (PII) is the costliest record type to be exposed in a breach on a per-record basis (around $150 per record). However, other corporate data (not containing PII) falls closely behind with average costs to businesses around $149 per record and intellectual

continued on page 11

continued from page 10

property data around $147 per record. Even anonymized customer data averaged $143 per record and employee PII averaged $141.

Data breaches also can take a heavy toll on a company's reputation—which ultimately impacts the bottom line in the form of lost business. The Ponemon/IBM report states: "Lost business costs accounted for nearly 40 percent of the average total cost of a data breach, increasing from $1.42 million in the 2019 study to $1.52 million in the 2020 study. Lost business costs included increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation."

Finally, data breaches can result in the loss of intellectual property. Around 32 percent of data breaches resulted in the loss of IP, which can have long-term repercussions on a company's well-being. While many think of credit card numbers as the only treasure sought by cyber attackers, many actually seek to obtain IP and other mission-critical strategic information.

As David Coher of Southern California Edison notes, even physical assets can be the target of a cyber-attack. If the device or system is connected to the internet, it has the potential to be hacked.

The Statutory Landscape

Current cybersecurity law is a patchwork of federal and state laws. On the federal level, Congress recently passed the IoT Cybersecurity Improvement Act of 2020. This new law establishes minimum security standards for the Internet of Things and connected devices owned or controlled by the Federal Government. The new law charges the National Institute of Standards and Technology with creating recommendations for secure development, identity management, patching and configuration management related to Internet of Things (IoT) devices. In addition, the act increases federal oversight for IoT security as administered by the Office of Management and Budget and the Department of Homeland Security.

At the state level, all 50 states and territories have their own data breach laws. Nearly all of them generically require organizations must maintain reasonable and appropriate security controls. However, in 2020, 38 states, plus D.C. and Puerto Rico, introduced cybersecurity-focused bills with more explicit standards for data and cyber security. Although few bills gained traction or were passed, lawmakers considered more than 280 state-level cybersecurity bills in 2020, demonstrating the heightened awareness of cyber risks and the need to legislate minimum standards.

Ideally, future cybersecurity legislation will continue to focus on flexibility, so that small businesses are not crushed by an onerous regulatory burden but organization of all sizes and sophistication are accountable for appropriate security programs, based on risk. HIPAA is a good model for this approach, demanding a high level of accountability from healthcare providers but not mandating exactly how they must implement these cybersecurity standards.

Risk Mitigation—Fighting Back

So what are company leaders to do? At-home working is not going away anytime soon, even once the pandemic ends. Nor are bad actors and nation-states looking to hack their way into unsuspecting victims' systems. Here are a few best practices:

- Take an inventory of all strategic assets and where they are stored. Creating such a data inventory can be both difficult and time-consuming, but it is vital. Once security professionals know where particular assets are kept within their organization, they can build layers of protections around them.
- Not every asset can be protected with the same level of diligence. The key is to focus on assets that will create the biggest problems if compromised.
- Assume that your organization will be impacted by a cyberattack and create an incident response plan as well as a disaster recovery and business continuity plan to mitigate the damage.
- Consider getting cyber insurance but make sure that the policy actually covers real-world cyberattacks and the damage they cause. Pay particular attention to exemptions and exclusions, as some insurers have changed how they handle such items, particularly in light of new liabilities during the pandemic.
- Third-party vendors, customers and business partners can be a source of cyber vulnerability, so ensure contracts include language that addresses liability and risk allocation.
- Employees are your biggest security vulnerability. Security training and education can be a relatively low-cost way to immediately improve an organization's cyber defenses. Training should be presented as a benefit to all and not a "trap" for employees not following company policy.
- Cybersecurity impacts all departments, so consider creating an organization-wide security team, with members from all departments, that meets regularly with the Chief Security Officer.

Once you have an incident response plan (including disaster recovery and business continuity components), it is equally important to test that plan and associated processes. Organizations should run "tabletop" exercises – a mock, organization-wide event for incident response purposes – and consider using an outside facilitator to give a fresh set of eyes and an independent perspective. Both Stephanie Lambert and David Coher stress that tabletops are one of the most important preventative measures and essential to ensuring your organization maintains an effective response plan.

A tabletop allows an organization to consider the thousand-and-one considerations that arise and decisions that must be made during a cyber event. For example, what if the organization's systems need to be completely shut down?

continued on page 12

continued from page 11

Who makes that decision, and what is the process for making and implementing that decision? Going through this type of mock scenario can help organizations be better prepared for a real cyberattack.

Assistant U.S. Attorney JoAnna McFadden stresses that getting the FBI involved early is important. The FBI has extensive experience with these attacks. Working with the FBI and a breach response team immediately can reduce the damage from the attack and increase the chance the attacked will be stopped or apprehended.

Company leaders also need to ensure that they allocate sufficient and appropriately qualified resources to cybersecurity, even during the current economic downturn. Around 62 percent of IT team leaders say their organization's cybersecurity team is understaffed, while 57 percent say they currently have unfilled cybersecurity positions on their team.

Conclusion

Cybersecurity has never been easy, and the challenges presented by the COVID-19 pandemic and work-from-home environment have exacerbated these difficulties. However, through a careful combination of legal compliance strategies and focused IT solutions, organizations can position themselves to guard against cyberattacks and mitigate the damage should one occur.

Author:

Tara Cho

Chair of Womble Bond Dickinson (US) LLP's Privacy and Cybersecurity Team, Tara's practice is dedicated to counseling clients on privacy and data security issues across industries such as technology, retail, e-commerce, healthcare/healthtech and life sciences, and she regularly provides guidance on matters related to the CCPA, CPRA, HIPAA, COPPA, CAN-SPAM, and other state and federal privacy, security and data breach laws in the U.S.

The Anti-Money Laundering Act of 2020: A Survey of Key Provisions and Practice Takeaways

By Barak Cohen, Tre A. Holloway, Jamie Schafer, Joseph P. Cutler, and Samuel D. Boro, Perkins Coie LLP

On New Year's Day 2021, Congress overrode a presidential veto to pass the Anti-Money Laundering Act of 2020 (AMLA 2020), which amends and modernizes the Bank Secrecy Act (BSA). The AMLA 2020 includes sweeping reforms updating and modernizing U.S. anti-money laundering laws, rules, and regulations. While most of these reforms target financial institutions subject to the BSA, several have broader implications for domestic and international business.

About the Series

This multipart series will highlight key takeaways from the AMLA 2020 with practical implications for our clients, including (1) new and expansive requirements for disclosure of corporate beneficial ownership, which the Financial Crimes Enforcement Network (FinCEN) is now actively working to implement; (2) enhanced incentives for whistleblowers to report money laundering violations; (3) expansion of U.S. subpoena authority over foreign financial institutions that maintain correspondent accounts in the United States; (4) new criminal penalties for concealing the involvement of senior foreign political figures and certain designated entities in transactions involving U.S. financial institutions; (5) expansion of AML law to codify jurisdiction over virtual currency activities; and (6) development of regulatory solutions with a greater focus on emerging technologies. Below is a high-level overview of some topics this series will cover:

New Beneficial Ownership Disclosure Requirements. Perhaps most significantly, the AMLA 2020 requires many corporations and limited liability companies (LLCs) to disclose their beneficial owners to the government—a new requirement that will apply to previously unregulated entities. The AMLA directs FinCEN to maintain a secure beneficial ownership registry of legal entities to facilitate investigations by law enforcement and diligence by financial institutions. This provision, aimed at shell companies and other single-purpose vehicles, is designed to discourage the use of anonymous entities to disguise the natural persons behind a corporation. On April 1, 2021, FinCEN issued an Advanced Notice of Proposed Rulemaking, setting out the questions it is grappling with in its effort to issue the required regulations by January 1, 2022, and soliciting comments from the public on how the beneficial ownership rule should be implemented. The first part of this series will describe the expanded statutory definition of "beneficial owner" and survey the AMLA's long list of exemptions to the registration requirements as well as discussing some of the key takeaways from FinCEN's recent public notice.

Significantly Enhanced Whistleblower Incentives. The AMLA 2020 introduces a whistleblower program modeled after the program used by the U.S. Securities and Exchange Commission. These provisions incentivize whistleblowers to report violations of the BSA and authorize increased monetary rewards for those who provide information to their employers or to the government. The availability of awards for internal reporting is a provision that may be particularly troublesome where the reporting employee and the company may disagree as to whether the conduct at issue must or otherwise should be reported to regulators. The second part of this series will discuss those provisions in detail.

continued on page 13

continued from page 12

Expanded Subpoena Authority. The AMLA 2020 expands the U.S. Department of Justice's subpoena authority over foreign financial institutions. It gives the secretary of the treasury and the attorney general authority to issue subpoenas to foreign financial institutions that maintain correspondent accounts in the United States with regard to any account records in their possession, a significant expansion from the prior authorization which was limited to records relating to U.S. correspondent accounts. The third part of this series will explain those new provisions and their implications for foreign financial institutions as well as foreign individuals and entities under investigation.

New Penalties for Concealing Transactions Involving Senior Foreign Political Figures. Finally, the AMLA 2020 amends the BSA to include criminal penalties prohibiting willful concealment from financial institutions of transactions involving senior foreign political figures and certain designated entities of money laundering concern. Most notably, the prohibition extends criminal penalties to anyone involved in the concealment, misrepresentation, or falsification (or attempted concealment, misrepresentation, or falsification) to a financial institution of material facts regarding the ownership or control of assets exceeding $1 million by a senior foreign political figure (or any immediate family member or close associate). The penalty gives sharp teeth to the transactional diligence process and will undoubtedly enhance the quality of diligence received by financial institutions vetting account holders and transactions. Like other recent anti-money laundering disclosure rules—such as the real estate-related global targeting orders that have been issued and continually expanded over the last several years—this may have important implications for expanding anti-corruption enforcement. This provision will be explored in the fourth installment of our series.

Expansion of AML Law to Codify Jurisdiction Over Virtual Currency Activities. The AMLA 2020 codifies prior FinCEN guidance that requires entities that conduct certain virtual currency business activities to register as money services businesses. By expanding the definitions of terms like "financial institution" and "money transmitting business" the new law includes businesses that exchange or otherwise transmit virtual currency or "value that substitutes for currency." FinCEN guidance was controversial in the industry, and its codification in statute will create additional challenges and opportunities.

Developing an Emerging Financial Technology Focus. The AMLA 2020 puts in place the impetus for financial regulatory agencies and the Government Accountability Office to conduct studies and provide reports to Congress and develop capabilities to better understand and adapt regulatory frameworks to address emerging fintech technologies. The law directs FinCEN to maintain emerging technology experts to identify emerging technologies such as artificial intelligence, digital identity technology, and distributed ledger technologies that may be able to assist the government and financial institutions to counter money laundering and terrorist financing. The federal financial regulators are directed to study emerging payment methods like virtual currencies and peer-to-peer payment systems and provide reports to Congress on their use in money laundering and illicit activities. The federal financial regulators have been advancing the use of emerging technologies by financial institutions, and the AMLA 2020 directs FinCEN to establish a no-action letter process, which provides the opportunity for the industry to better understand the technology solutions acceptable to regulators for BSA compliance.

Authors:


Barak Cohen

Barak Cohen, a partner in Perkins Coie's White Collar & Investigations practice, lead for commercial litigation in the firm's Washington, D.C., office, chair of Perkins Coie's firmwide Cannabis industry group, helps companies and individuals, particularly in highly-regulated industries, such as healthcare, respond to inquiries from diverse government agencies and legislative bodies, such as the DOJ, the Department of Health and Human Services (HHS), Consumer Finance Protection Bureau (CFPB), Congress, state legislative committees, and federal agency inspectors general.


Jamie Schafer

Jamie Schafer, a partner in Perkins Coie's White Collar & Investigations practice, represents both corporations and individuals in complex U.S. and cross-border criminal and regulatory matters, and also regularly conducts internal investigations focusing on a broad range of potential misconduct.


Joe Cutler

Joe Cutler, a partner in Perkins Coie's Privacy & Data Security practice, helps evaluate the regulatory exposure and compliance paths for emerging distributed ledger technology companies, cryptocurrency exchanges and token-based projects and helps companies navigate the regulatory thickets surrounding token sales, digital and self-sovereign identity, IoT/AI/blockchain convergence and the business of blockchain.


Sam Boro

Sam Boro, a counsel in Perkins Coie's Technology Transactions & Privacy practice, counsels clients, including banks, fintech companies, financial services firms and credit card companies, on payments processing, consumer protection, business operations, government investigations and regulatory compliance.


Tre Holloway

Tre Holloway, an associate in Perkins Coie's Business Litigation practice, assists clients in a wide variety of matters, both civil and criminal, at all stages of state and federal litigation, and his practice focuses on all phases of complex commercial disputes, white collar, antitrust, and political law.

The missing link in whistleblower programs – the escalation protocols

By Brett Ingerman, DLA Piper

In the world of corporate compliance, companies around the world are particularly focused on their whistleblower programs. It is beyond best practices to have an effective whistleblower hotline, including anonymous reporting (where permitted), non-retaliation pledges, robust investigation and remediation, and plenty of training and awareness campaigns. Companies are spending significant resources analyzing their hotline data, looking for trends and putting in place risk mitigation strategies. But recent experience says that many companies are missing a vital part of their whistleblower program – escalation protocols.

Escalation protocols are the rules or guidelines for how to handle a complaint once it's been lodged – whether through the hotline, in an email to a board member, or orally from a vendor to an employee. What happens next? Who gets notice, when and how? How is it investigated and by whom? How and when does the attorney-client or some other privilege attach? How do you communicate with the reporter and what do you say? These are all important questions that, if answered incorrectly, could lead to significant regulatory, civil and in some circumstances criminal risk. Yet they are questions easily answered by referring to a fixed set of escalation protocols.

Escalation protocols should include the following, at a minimum:

- Intake, notice and assignment – The first protocol should deal with the intake of the complaint, who gets notice of the complaint, and which department will be responsible for its investigation. The majority of complaints will be received directly via the hotline, but directors, officers, vendors and employees who receive complaints should be instructed to immediately enter them into the hotline system. The hotline system then should immediately notify the legal department and at least one other department, usually human resources or compliance. Designated individuals from those departments would then determine whether additional notice was required based on the nature and severity of the complaint (ie, senior executives, board members). The escalation protocols should lay out generally the criteria for providing notice for different types of complaints. Once notice is provided, the legal department should determine who will investigate. Investigator options include legal, compliance, human resources, security or some combination thereof. Consideration also should be given to bringing in outside counsel or other external consultants, including media relations. But having legal do the initial assessment of who should investigate allows the company to assert attorney-client privilege over those communications.
- Investigation – Once it is determined who will conduct the investigation, the company should have investigation protocols that describe how to conduct the investigation. The investigation protocols ensure that each investigation is performed properly, fairly, consistently and, where appropriate, subject to the attorney-client privilege. Investigation protocols include: (1) developing an investigative plan; (2) setting a time frame; (3) preserving and reviewing documents and electronic data; (4) conducting interviews; (5) reporting; (6) disclosures; and (7) discipline and remedial measures. Recent Department of Justice guidance on corporate compliance programs recommends periodic audits of compliance investigations to ensure consistent approach and discipline.
- Communicating with the reporter – The escalation protocols also should describe how and when to communicate with the person who reported the complaint. These communications ensure the reporter is confident that the company is taking the allegations seriously, and may well prevent the reporter from reporting the complaint to an external regulator. Proper communication also promotes a culture of compliance and empowers employees to report incidents of wrongdoing.
- Remediation – It is now best practice for remediation to be a part of the escalation protocols. This means that all complaints should be designated as "closed without further action" or "closed with remediation." The remediation should be documented and then fed into a compliance risk assessment or internal audit plan so that it can be audited during the next audit cycle. Again, recent DOJ guidance recommends a "Lessons Learned" approach that ensures a company learns not only from its past compliance missteps, but also from compliance failures at peer companies and relevant markets.

Putting escalation protocols in place is an easy and effective way to ensure that a whistleblower program functions efficiently and, perhaps more importantly, enjoys the protection of the attorney-client privilege where appropriate. There are countless horror stories of companies facing civil litigation or regulatory inquiries where the mishandling of complaint intake has led to the production of bad documents, resulting in heavy fines, settlements and jury verdicts. Mitigate those risks through carefully crafted escalation protocols. And remember: there is no one-size-fits-all. Every company will have its own view on how to handle whistleblower complaints. Escalation protocols ensure they are handled properly, consistently, fairly and confidentially.

Author:

Brett Ingerman

Brett Ingerman is the managing partner of DLA Piper's Baltimore office. His primary areas of practice are business and commercial litigation and arbitration, with a focus on complex commercial disputes, insurance and bankruptcy litigation. He has tried numerous cases to verdict in courts all over the country.

Brett also has significant experience in corporate investigations, governance and compliance involving criminal, quasi-criminal and administrative agencies. He has designed and implemented global compliance programs for companies large and small, and focuses on providing practical compliance advice consistent with best practices and local custom.

Hart-Scott-Rodino Antitrust Improvements Act- A Robust Compliance Program May Prevent HSR's Aggregation Rules from Becoming A Trap for the Unwary

By Colleen Pleasant Kline, Denise Gunter, and Carrie Hanger, Nelson Mullins

If you have engaged in any equity or asset transaction, merger or other form of a consolidation or joint venture, you may already be familiar with the Hart-Scott-Rodino Antitrust Improvements Act of 1976 (the "HSR Act") and its accompanying rules found in 16 CFR 801-803. The Act and the rules require certain acquirers and targets (and the persons who control them) to file a detailed notice with the Federal Trade Commission ("FTC") and the Department of Justice ("DOJ") prior to completing the transaction or risk facing substantial penalties or fines. The HSR rules are complex and nuanced, and determining whether an HSR filing may be required is a very fact specific process focusing on the underlying transaction, the parties to it and their ultimate parent entities. Under the HSR Act, certain transactions, which exceed the minimum size of transaction threshold (currently $92 million), may trigger a filing requirement if the parties to the transaction otherwise meet the applicable size of person test and no other exemptions apply. *(See Key Updates: New, Lower HSR Notification Thresholds for current thresholds.)* For larger transactions, i.e., those currently valued at greater than $368 million, the size of person test does not apply. If an HSR filing is required, the parties to the transaction must wait until the expiration of the waiting period (30 days) before they may proceed with the closing on the sale.

What many corporate counsel and their clients are surprised to learn is that the HSR Act's aggregation rules, found at 16 CFR 801.13, 810.14 and 801.15, may trigger a filing in smaller transactions when existing holders of voting securities, assets or non-corporate interests seek to increase their stake in an entity. For example, any of the following may potentially trigger HSR reporting requirements: (i) the sale of additional voting securities in an equity round to an existing shareholder, even though the total value of the round and the investor's proposed investment are below the applicable size of transaction; (ii) the exercise of warrants or convertible notes; (iii) private sales of existing voting securities among existing equity holders (e.g., transactions that are not part of a financing round); (iv) additional acquisitions of assets from the same ultimate parent entity within a specified time frame; and (v) the exercise of certain stock options, stock appreciation rights and similar equity incentive compensation to certain officers or directors. Additionally, certain changes in the roles of equity holders who previously fell under an existing exemption that did not require a filing, such as the investment exemption, may also trigger a filing. For example, a filing may be triggered when a passive investor holding less than 10% of the voting securities of an issuer either (i) becomes active in management and/or (ii) due to other equity activities within the issuer holds more than 10% in the issuer. This article examines some of the common issues that arise when current investments are aggregated with future investments, and ways that corporate counsel can ameliorate the risk of missing a filing obligation.

The Basics of Aggregation

Let's begin with a relatively straight forward example: Corporation X, which does not currently own any part of Target B or Target B's controlled entities, enters into a letter of intent to acquire a combination of voting securities and assets from Target B, as well as Target B's controlling interest in LLC Z, all in the same transaction. It is logical to aggregate the value (as determined pursuant to 16 CFR 801.10) of each of item being acquired in a single transaction to determine whether a filing may be required, and that is exactly what the HSR rules require. See 16 CFR 801.13. But what if Corporation X first acquired voting securities from Target B, and then at some later point, acquired additional voting securities, assets or non-corporate interests from Target B? The aggregation rules at 16 CFR 801.13 – 801.15 establish a number of rules and exceptions to these rules, some of which may seem like brain teasers. To aggregate or not will depend on several factors, such as what is being acquired, the order in which it is acquired and timing.

To keep the reader from developing a headache, let's continue with Corporation X which already owns voting securities in Target B, and proposes to buy more voting securities from Target B. An acquiring person who is also an existing shareholder may trigger a reporting requirement if the value of the voting securities that such acquiring person held prior to the acquisition when aggregated with the value of the voting securities to be acquired is greater than $92 million, or the next relevant HSR notification threshold, and no other exemptions apply. See 16 CFR 801.13(a). It is therefore possible for the unwary shareholder to trip a reporting requirement by acquiring even a small number of voting securities through any of the ways noted above. The risk for issuers that have equity holders who are entities or affiliated entities is compounded where the ultimate parent entity (as defined in the HSR rules and discussed below) of those affiliated entities, if the same, may "hold" voting securities through multiple equity holders within the issuer. If such newly acquired voting shares were not part of any prior HSR filing or included within an initial HSR filing (for purposes of any contemplated equity earn-outs or other convertible securities), but the subsequent acquisition of additional voting shares would cause such person to hold voting securities in excess of the next reporting threshold from that in the original filing, an HSR filing may be required. Additionally, if the prior HSR filing was more than 5 years from the new issuance, a new HSR filing may also be required. See 16 CFR 802.21(a)(2).

continued on page 16

continued from page 15

Note, however, that a mere increase in the value of an investment will not by itself trigger a filing; rather, the investor must add to its holdings in order to trigger a filing. For example, if Corporation X acquired $80 million worth ofTarget B's voting securities in 2019, and the value of that investment increased to $92.1 million in April 2021 without Corporation X doing anything, Corporation X would not have a filing obligation. Now assume one change in the facts: in April 2021, Corporation X buys additional shares of Target B's voting securities. If the size of person tests are satisfied and no exemptions apply, Corporation X and Target B may have a filing obligation. In the latter case, Corporation X took an affirmative step to increase its investment inTarget B. Let's further assume the value ofCorporation X's investment was $85 million in April 2021 and Corporation X proposes to buy an additional $7.1 million worth oTarget B's voting securities. Again, a filing may be required because Corporation X seeks to increase its holdings inTarget B. In the foregoing examples, we have internationally described the securities as "voting securities." As the HSR Act and its accompanying rules make clear with respect to securities, HSR applies only to voting securities, which is a defined term under 16 CFR 801.1 (f)(1)(i) ("any securities which at present or upon conversion entitle the owner or holder thereof to vote for the election of directors of the issuer, or of an entity included within the same person as the issuer."). So, understanding exactly what is being bought and sold (voting securities versus non-voting securities) is critically important.

Non-corporate interests get special treatment in HSR. Holdings in non-corporate entities include partnerships and limited liability companies. See 16 CFR 801.1 (f)(1)(ii). For purposes of HSR, non-corporate interests only matter when their acquisition confers "control" over the non-corporate entity. See 16 CFR 801.10(d); 801.13(c)(2). For example, assume Corporation X owns voting securities of Target B, and later proposes to buy a *controlling* interest in LLC Z, a non-corporate entity which Target B controls. Corporation X must aggregate the value of the voting securities it already owns with the value of the non-corporate interests in LLC Z. The answer would be different if Corporation X proposes to acquire a *non-controlling* interest in LLC Z. In that case, no aggregation is required. See 16 CFR 801.13(c)(2).

With respect to the aggregation of assets, the rules differ slightly in that the aggregation of assets has a timing aspect which is not applicable in the aggregation of voting securities or noncorporate interests. In the event that an acquiring person has acquired assets from the same acquired person, and within 180 days, executes a letter of intent or an agreement in principle to acquire additional assets from the same person, then the parties to the transaction must aggregate the assets to be acquired with the assets already acquired. 16 CFR 801.13(b)(2). Note that the Premerger Notification Office ("PNO") of the FTC has taken the position that aggregation is appropriate in certain circumstances that do not strictly comport with the above facts, if the circumstances suggest that the parties may be employing a device for intentionally avoiding an HSR filing. (See 16 CFR 801.90).

To illustrate the nuances of HSR, the order in which one acquires assets matters greatly. For example, assume Corporation X owns voting securities of Target B, and then subsequently proposes to acquire assets from Target B. The parties must aggregate, unless they previously filed HSR on the prior voting securities acquisition, or the transaction was exempt under 16 CFR 802.21. See 16 CFR 801.13(a)(3)(i) and (ii). But what if the transaction was done in reverse order, and Corporation X first acquired assets from Target B, and within 180 days signs a letter of intent proposing to acquire voting securities from Target B? In that case, the parties would not aggregate. See 16 CFR 801.14, and example 2 thereunder.

The foregoing examples are not exhaustive. The HSR rules are complex and not necessarily intuitive. Unfortunately, the stakes are high for not getting it right. If a subsequent acquisition would have required an HSR filing and the parties failed to file, the issuer and the acquirer are subject to potential fines and penalties which can be significant. The parties would also be required to file a corrective HSR filing and explain why the filing was missed and the steps the parties have taken to prevent this from happening in the future.

Ways to Manage HSR Risk

How then can corporate counsel manage their HSR risk in light of the aggregation rules? First and foremost, a robust HSR compliance program is critical. Both buyers and sellers have HSR obligations, so it pays to stay up to date on your client's investments and your client's investors. As discussed later in this article, a tracking system can be very helpful in managing the complexities of HSR's aggregation rules. The aggregation of subsequently acquired assets is usually an easier risk to mitigate if corporate counsel identifies whether additional assets are being acquired from a previous seller. It can then look to see if the subsequent acquisition should be aggregated.

For purposes of managing the risk related to aggregation of voting securities and noncorporate interests, corporate counsel must first determine who controls the relevant target and the acquirer. "Control" is defined under 16 CFR 801.1(b) means: (1) *EITHER* (i) holding 50 percent or more of the outstanding voting securities of an issuer or (ii) in the case of an unincorporated entity, having the right to 50 percent or more of the profits of the entity or the right to 50 percent or more of the assets of the entity in a dissolution; or (2) having the contractual power presently to designate 50 percent or more of the directors of a for-profit or not-for-profit corporation, or 50 percent or more of the trustees in the case of trusts that are irrevocable and/or in which the settler does not retain a reversionary interest. Note that the FTC is currently proposing changes to these rules which may alter the definition of control as it relates to certain private equity funds or master

continued on page 17

continued from page 16

limited partnerships in particular. (See *Key Updates: On the Horizon: Proposed Changes to the Definition of Control.*) As part of this review, the parties look at who ultimately "controls" the acquirer (and the acquired person) until no one person or entity "controls" it, and that person or entity is the "ultimate parent entity" for HSR purposes. Then, the parties look at all voting securities, non-corporate interests and assets (as applicable) that the ultimate parent entity holds and all entities within the ultimate parent entity holds for this analysis.

Once corporate counsel understands who "controls" certain entities, or at a minimum, who the affiliated equity holders are, managing the risk related to the aggregation of noncorporate interests is currently also easier (although subject to change). If an equity holder (or the affiliated equity holder(s)) will hold 50% or more of the noncorporate interests entitling that person to 50% or more of the profits from operations or 50% or more of the assets on dissolution, then that person is deemed to "control" the noncorporate entity. 16 CFR 801.1(b).

Mitigating the risk for voting securities requires a more robust compliance protocol, particularly for a privately held company. As the underlying issuing company's enterprise value grows to approach the lowest notification threshold triggering filing, it should establish a tracking system to monitor the number of shares held by officers, directors, and other significant shareholders, including the HSR market value of the equity held. The issuer should also request regular details regarding affiliated shareholders to ascertain whether as part of this tracking system, one or more affiliated entities should be aggregated together. (It is also acceptable to presume for monitoring protocols that affiliated entities should be aggregated as one entity if those parties are reluctant to provide ownership details on a regular basis). The issuer then should notify those persons that hold directly or indirectly voting securities or noncorporate interests in the issuer that are (for example) within 75% of the value of a notification threshold; and advise them that subsequent acquisitions may trigger an HSR filing requirement.

In the event that such equity holder's holdings already exceeded a notification threshold due to market appreciation, such person should also be given notice of potential HSR obligations. Any transaction involving an acquisition of additional voting securities or noncorporate interests, as applicable, to which the issuer is a party should be explicitly conditioned upon the satisfaction of any HSR Act obligations, or upon receipt by the issuer of advice from experienced HSR counsel that no notifications are required to complete the transaction. Getting in front of the situation is key to avoid surprise and potentially delaying a transaction.

Additionally, once the issuer is approaching or has exceeded a notification threshold at an enterprise value, the issuer may want to consider adding standard conditions to exercise or purchase that such exercise is subject to expiration of all applicable notification and waiting periods under the HSR Act and may want to include such a term in any of its shareholder agreements. Issuers should also apprise equity holders who may be approaching the threshold that they should review the aggregation rules even if they are acquiring voting securities from other equity holders in private sales, as the acquisition of voting securities in private sales are also subject to the aggregation rules discussed herein and may also trigger a reporting requirement.

Certain Key Updates on HSR

1. Temporary, Indefinite Suspension of Early Termination.

On February 4, 2021, the FTC and DOJ announced that they have temporarily suspended the practice of granting early termination of the statutory initial waiting period associated with HSR filings (30 days for most transactions; 15 days for cash tender offers and bankruptcies) when the transactions do not raise antitrust concerns. The stated reasons for this suspension are a change in administrations and a sharp increase in the number of filings. While we expect that the suspension of early termination will not be permanent, it is unknown when the agencies will resume the practice of granting early termination. This means that clients should plan to wait the full statutory waiting period (typically, 30 days) after making an HSR filing before closing. On March 12, the FTC further clarified that it will grant early termination in two related and narrow circumstances: 1) when a transaction is already being investigated (i.e., a Second Request has been issued), and the parties address the agencies' concerns about their transaction without substantially complying with the Second Request; and 2) when a Second Request has been issued, and the parties negotiate a Consent Agreement (i.e., a Settlement Agreement) to resolve the agencies' concerns about their transaction.

2. New, Lower HSR Notification Thresholds.

For the first time since 2010, the HSR notification thresholds have been lowered as result of the decline in the gross national product in 2020 due to the pandemic. These new thresholds went into effect on March 4, 2021, and are summarized as follows:

Test	2021 Threshold (effective March 4, 2021)(in USD)
Minimum Size of Transaction For Filing Where the Size of Person Test is Met	$92 million
Size of Person (one party must meet this lower threshold)	$18.4 million
Size of Person (one party must meet this higher threshold)	$184 million
Size of Transaction Where Size of Person Test Does not Apply	$368 million
Filing fee: $45,000	Transaction value: More than $92 million but less than $184 million
Filing fee: $125,000	Transaction value: More than $184 million but less than $919.9 million
Filing fee: $280,000	Transaction value: More than $919.9 million

continued on page 18

continued from page 17

Generally, and unless an exemption applies, HSR will apply to transactions where the size of transaction and size of person tests below are met, although for larger transactions, only the size of transaction test applies.

Notification thresholds for aggregation for additional reporting requirements for assets, voting securities and noncorporate interests are

1. Aggregated value: More than $92 million but less than $184 million
2. Aggregated value: More than $184 million but less than $919.9 million
3. Aggregated value: More than $919.9 million

For the aggregation of voting securities:

1. Holding 25% of the voting securities of any issuer, but less than 50%, valued at greater than $1,839.8 billion; OR
2. Holding 50% of the voting securities of any issuer, valued at $92 million or more.

In addition, HSR penalties have also been adjusted slightly upward, from a daily penalty of $43,280 to $43,792. HSR filing fees, which are based on the size of transaction, have not been increased, and the existing three-tiered filing fee structure remains in place for 2021.

3. On the Horizon: Proposed Changes to the Definition of Control.

The FTC, with the concurrence of the DOJ, has also proposed changes to the HSR rules that will significantly increase the number of filings required by investment funds and master limited partnerships ("MLPs"). The proposed changes would revise the HSR definition of "person" to include "associates" (entities under common investment management but not common HSR control). If adopted, this revised definition would require investment funds and MLPs to aggregate their holdings across commonly managed funds and entities when determining whether the size of transaction test and size of person tests are met. In other words, associated funds that each qualify as its own "ultimate parent entity" and individually hold less than $92 million worth of an issuer's voting stock are currently not required to file HSR even if they collectively hold more than $92 million of the issuer's voting stock. Under the proposed rule, a filing would be necessary unless an exemption applies. The proposed changes would also add a new de minimis exemption for acquisitions of 10% or less of the voting securities of an issuer provided that the acquiring person does not have a "competitively significant relationship" with that issuer. Comments to the December 1, 2020 Notice of Proposed Rule Making were due on February 1, 2021. Several sets of comments were filed, and the FTC and DOJ have not yet provided any additional information as of this April 26, 2021. If an issuer has investment funds or MLPs as equity holders, the issuer and its counsel should be aware that HSR may become applicable and that these rules will likely alter how transactions and additional aggregation is analyzed.

Conclusion

If your company is actively engaged in merger and acquisitions activity, you should consider developing a robust HSR compliance program if you do not already have one in place. A compliance program will help you manage your HSR risk including avoiding missing a filing obligation under the complex aggregation rules. Parties who are interested in adopting compliance programs to mitigate HSR risk, are encouraged to work with experienced HSR counsel in light of the pending rule changes. Both issuers and other corporate counsel are encouraged to seek the subject matter expertise of HSR attorneys in evaluating transactions where a reporting threshold may be reached or in those transactions involving existing equity holders.

Authors:

Colleen Pleasant Kline is a Partner in the Baltimore, Maryland office of Nelson Mullins. She advises and represents buyers and sellers in mergers and acquisitions, capital raises and other corporate attorneys on compliance with the Hart-Scott-Rodino Antitrust Improvements Act of 1976. She may be reached at 443-392-9411 or colleen.kline@nelsonmullins.com.

Colleen Pleasant Kline

Denise Gunter

Carrie Hanger

Denise Gunter and **Carrie Hanger**, partners in Nelson Mullins' Winston-Salem, NC office, assisted with this article. Denise Gunter may be reached at 336-774-3322 or denise.gunter@nelsonmullins.com. Carrie Hanger may be reached at 336-774-3327 or carrie.hanger@nelsonmullins.com.

This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Board Leadership

President
Dan Smith
Under Armour
daniel.smith@underarmour.com

President Elect
Kimberly Neal
General Counsel
The Children's Guild, Inc.

Immediate Past President
Larry Venturelli
Zurich North America
410.559.8344
larry.venturelli@zurichna.com

Treasurer
Kimberly Neal
General Counsel
The Children's Guild, Inc.
NealK@ChildrensGuild.org

Secretary
Taren Butcher
Allegis Group
tbutcher@allegisgroup.com

Program Chair
Matthew Wingerter
Catholic Relief Services
matthew.wingerter@crs.org

Board Members
Cory Blumberg
Taren Butcher
Dee Drummond
Joseph Howard
Raissa Kirk
Kimberly Neal
Danielle Noe
Shane Riley
Dan Smith
Kristin Stortini
Larry Venturelli
Michael Wentworth
Matthew Wingerter

Past Presidents Advisory Board
Prabir Chakrabarty
Karen Gouline
Melisse Ader-Duncan
Frank J. Aquino
Ward Classen
Maureen Dry-Wasson
Lynne M. Durbin
Lynne Kane-Van Reenan
Andrew Lapayowker
William E. Maseth, Jr.
Christine Poulon
Dawn M. B. Resh
Mike Sawicki

Chapter Administrator
Lynne Durbin
ldurbin@inlinellc.net