Inside 2Q2017

ACC Association of Corporate Counsel

BALTIMORE

FOCUS

President's Message

Christine Poulon

Welcome to a new year Baltimore Chapter Members! At the start of the calendar year, I began my tenure as the Chapter President, and I am looking forward to working with you in my new capacity.

We have great programs scheduled for the year. We have already had updates on labor and employment, immigration, health care and tax law, and we have lunches with topics including the False Claims Act, intellectual property and more. And, we have a new Spring/Summer Social this year hosted by our now Premier sponsor Womble Carlyle.

In our next newsletter we'll have an update on our signature Golf Spa event held May 15th.

Thank you to all the people that responded to our Chapter survey - we had a fabulous response rate with close to 35% of our almost 300 members responding. Some things that we learned from the survey include:

- most of the respondents appreciate the educational programs and nearly half like the networking opportunities;
- there is interest in skills development programing (such as contract drafting and negotiation, project management) but also in the areas of corporate law and governance, ethics and compliance, employment law and information security and privacy; and
- nearly 90% of those responding had attended at least one event in the past year

We will work to bring you more topics that got the most votes. And we will look to engage those of you that are too far or too busy to attend our current programs and events. If you didn't get a chance to respond to the survey we are always open to feedback and suggestions - grab one of the Board members at lunch or send us an email.

We hope those of you who participated enjoy the $15 Amazon card!! Many thanks to our survey committee - Ed Paulis, Kaidi Isaac and Dana Gausepohl.

As we progress through this new year with new challenges we hope that you participate in the activities that we plan for you in the Baltimore area - whether that is a break from the office to attend a monthly lunch or some networking at a social event.

As always we'd like to thank our sponsors:

Premiere—Womble Carlyle and Miles & Stockbridge.

Gold—Kramon & Graham; Jackson Lewis; Saul Ewing; Whiteford, Taylor & Preston; DLA Piper and Anderson Kill.

Silver—Gordon Feinblatt, Corporation Services Company and The Lucas Group.

I leave you with a quote I recently read attributed to Marie Curry: "Nothing in life is to be feared, it is only to be understood. Now is the time to understand more, so that we may fear less." Let's move into this year with less fear and lots of understanding!! And if there's a legal issue you don't understand, let us know and we can make it the topic of the next luncheon!

And, if you ever want to share any other ideas or comments with the board, here is the current list of officers and directors:

Christine Poulon—President

Karen Davidson—President-elect and Treasurer

Ed Paulis—Secretary

Joseph Howard—Program Chair

Kaidi Isaac—Communications Chair

Dee Drummond—Day of Service Chair

Cory Blumberg—Golf/Spa Chair

Matthew Wingerter—Law School Outreach Chair

Dawn Resh—Immediate Past President

Larry Venturelli

Whitney Washington

Dana Gausepohl

Arielle Harry-Bess

Joal Barbehenn

Prabir Chakrabarty

ACC addresses law firm information security

By Mary Blatch, Director of Government & Regulatory Affairs, ACC

Unless you've been hiding under a rock, you know that law firms have been scrambling over the past few years to enhance their information security systems.

In-house counsel who are responsible for retaining outside counsel have also been putting in processes to evaluate their firms' information security protections. To assist in this task, ACC has developed a new resource to aid in-house counsel in setting information security expectations for their law firms and legal vendors.

Law firms: Attractive Targets

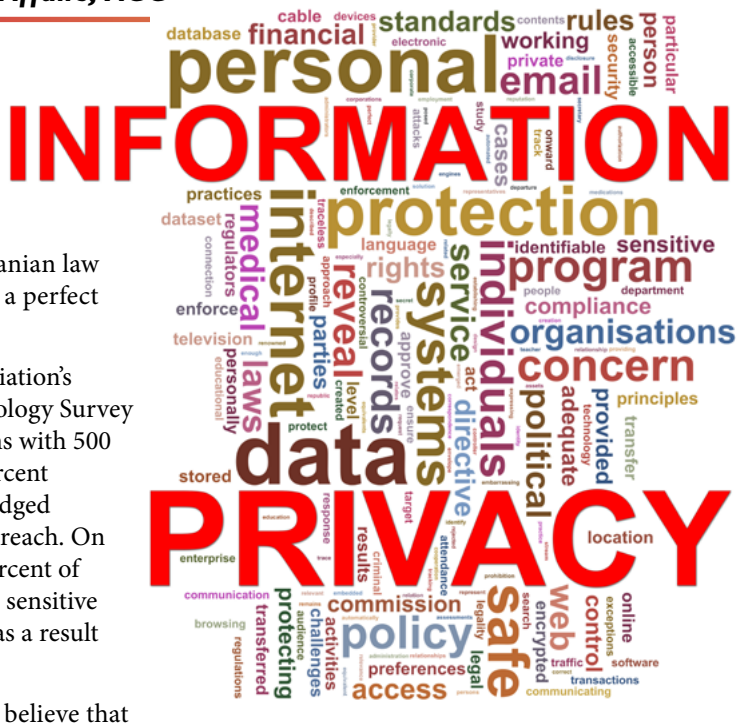
The attention to law firm information security over the past few years started when the FBI issued specific warnings to the legal sector that law firms are attractive "soft targets" for cybercriminals and that firms need to invest more in information security.

As an example of the types of threats that law firms are facing, in 2016, the FBI warned firms that a known criminal had been seeking a hacker to target many of the US's largest firms to gain access to information to be used for insider trading. The criminal offered to split proceeds of the crime with the hacker 50-50.

While many in-house counsel are addressing their own company's information security issues, law firms have come to be recognized as a potential "weak spot" in the data chain for two primary reasons.

The first reason is that until recently, law firms had not invested in their technology infrastructure to keep up with new developments in information security. For example, in a 2016 survey conducted by the International Legal Technology Association (ILTA) LegalSec, 65 percent of the 180 law firms surveyed had no personnel solely dedicated to information security.

The second reason is that law firms have been recognized as attractive targets for cybercriminals. Law firms store a large quantity of documents with highly sensitive and confidential information from many clients. With one penetration, a criminal can find information about many corporate targets. The leaking of documents from Panamanian law firm Mossack Fonseca is a perfect example.



The American Bar Association's most recent Legal Technology Survey revealed that among firms with 500 or more attorneys, 26 percent of respondents acknowledged experiencing a security breach. On the bright side, only 2 percent of those firms reported that sensitive client data was accessed as a result of the breach.

Of course, many experts believe that the number of breaches is actually much greater, it's just that the law firms do not know they have been breached.

So what does this mean about the current state of law firm information security? Increased awareness of the issue means that more law firms are investing resources in their technology infrastructure, but in-house counsel still need to hold their law firms accountable as stewards of their clients' information.

Setting expectations

It can be difficult for in-house counsel to determine reasonable expectations to hold a law firm to regarding information security. A recently released ACC resource should provide in-house counsel some assistance in that regard.

ACC's *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information* ("Model Controls") is a document in-house counsel can use as they set expectations with their law firms and other legal vendors, regarding the types of cybersecurity controls outside counsel should employ to protect their clients' confidential information.

The Model Controls project arose from the recognition among many ACC members that providing some consistency and a baseline understanding between law firms and their clients would be helpful so that companies and firms can work together to combat information security threats.

The Model Controls were developed by members working for companies in a variety of industries and of different sizes. The ACC working group also received input from law firms.

The document is meant to be customizable to members' particular circumstances. Working group members have already begun incorporating the document into their outside counsel guidelines. A Word version of the document is available to ACC members in ACC's Resource Library by searching "model controls."

By publicizing the Model Controls outside the ACC membership, ACC hopes that the Model Controls recommendations become widely used by in-house counsel. This will offer in-house counsel a streamlined and consistent approach to setting expectations with respect to the

continued on page 3

continued from page 2

data security practices of their outside vendors.

The Model Controls address 13 areas of cybersecurity controls, including data retention and destruction, data handling and encryption, data breach reporting, physical security, employee background screening, and cyber liability insurance. Some specific provisions include:

Requiring outside counsel to return or destroy client information once the information is no longer needed;

A 24-hour data breach notification requirement;

Encryption of data that is in transmission or being stored;

Requiring law firms to perform background checks on lawyers and staff;

Maintaining at least $10 million in cyber liability insurance.

In-house counsel should be particularly interested in the recommendation regarding notifying a client of a data breach. The Model Controls suggest a relatively short notification period of 24 hours.

According to Brennan Torregrossa, vice president and association general counsel at GlaxoSmithKline, who was involved in the working group that drafted the controls, "In the event that a client's data is compromised, this is not a time for there to be any misunderstanding that leads to a lack of communication between law firm and client. Trust is gained by protecting client data, but it also can be gained by being open, transparent, and cooperative when things go very wrong."

For in-house counsel and companies that have not yet started a process of vetting their law firms' information security practices, the Model Controls can be an excellent starting point. But the Model Controls should not be considered a definitive set of standards to be applied across all engagements and all law firms.

For example, the Model Controls may not provide adequate security protections for a business associate subject to HIPAA, and they may be more than is necessary for a firm handling a matter that does not involve receipt of much client confidential information.

Each law firm and client should use their own judgment and analysis to modify the Model Controls given their particular relationship, business needs, technology used and type of information being shared. And of course, if firms do not have some of the recommended practices in place, there may be a cost to implementing them.

Another consideration for in-house counsel in using the Model Controls is the extent to which the client itself meets the information security precautions recommended in the Model Controls.

Many of the recommendations in the Model Controls came from the policies of the working group members' companies, so these are practices that are common in corporate organizations as well.

One firm evaluating the Model Controls noted that the standard companies set for outside counsel should be consistent with the company's own standard. That likely depends on the risk profile of your company as compared to the law firm, but the point is a good one.

As in-house counsel and outside counsel continue to be so greatly affected by the threat of cybercrime, it is likely that standards for information security will be raised across the board.

Because information security practices will continue to evolve, the working group that created the Model Controls intends to periodically update the document. If you have feedback on the document, please contact Mary Blatch, ACC's director of advocacy and public policy at *m.blatch@acc.com*.

ACC News

ACC Annual Meeting: Exclusively for In-house Counsel

The 2017 ACC Annual Meeting, the world's largest gathering of in-house counsel, is scheduled for October 15-18 in Washington, DC. In less than three days you can choose from over 100 substantive sessions to fulfill your annual CLE/CPD requirements, meet leading legal service providers and network with your in-house peers from around the world. Visit *am.acc.com* to view full program schedule.

New to In-house? Are you prepared?

The ACC Corporate Counsel University® (June 14–16, New Orleans, LA), combines practical fundamentals with career building opportunities, which will help you excel in your in-house role. Come to this unrivaled event to gain valuable insights from experienced in-house counsel, earn CLE/CPD credits (including ethics credits) and build relationships and expand your network of peers. Register at *ccu.acc.com*.

Second Tuesday Webcast Series

Save the day for the second Tuesday of every month to learn about ACC online resources and how to maximize the value you receive from your membership. We will demonstrate how to identify and act upon key in-house legal practice trends and emerging law department issues, and access the knowledge and expertise of thousands of in-house counsel through benchmarking data, policy and contract templates, best practices, and other legal materials across key practice areas. Register today at *www.acc.com/SecondTuesday*.

continued on page 4

continued from page 3

Drive Success with Business Education for In-house Counsel

To become a trusted advisor for business executives, it's imperative for in-house counsel to understand the business operations of your company. Attend business education courses offered by ACC and the Boston University Questrom School of Business to learn critical business disciplines and earn valuable CLE credits:

- Mini MBA for In-house Counsel, June 5 – 7, Sept. 12-14, and Nov. 7 -9
- Finance and Accounting for In-house Counsel, Sept 25-27
- Project Management for in-house Law Department, Nov 13-14

Learn more and register at *www.acc.com/businessedu*.

Law Department Leadership 2.0 is coming to Montreal

Law Department Leadership 2.0 is back and coming to Montreal for the first time on 18 September. This popular program will provide you with the skills you need to be an effective leader in your company. Sessions will focus on getting the most out of your team, selling your ideas to senior management, trends in the in-house market, and essential project management skills for in-house leaders. Register today at *www.acc.com/ldl*.

Get fast, easy access to the practical answers and information you need to advise on a broad range of topics with General Counsel NAVIGATOR™ (GCN). GCN provides authoritative content, expert analysis, practical tools, primary law and more, in a single platform. ACC Members receive a complimentary add-on with your GCN subscription. For more information, visit *wolterskluwerlr.com/GCN* or call 1-877-324-6921.

Defensible deletion of email and other data is the most effective way to reduce risks and costs associated with data breach and e-discovery. ACC Alliance Partner Jordan Lawrence offers a cost-effective solution to ensure your records retention program is defensible, enforceable, and effective. Visit *www.jordanlawrence.com* or call 1-636-821-2222.

Demystifying Phantom Equity

By Paolo Pasicolan, Counsel, Miles & Stockbridge

Phantom equity is a colorful term for a simple concept: compensation that rewards key contributors for increasing the value of a company without the immediate issuance (or even any future issuance) of equity securities. Many companies grant phantom equity because it offers many of the risks and rewards of owning the company without most of the hassles of actual ownership. Here is a brief Q&A on how phantom equity works:

What is phantom equity?

Phantom equity is incentive compensation designed to mimic the benefits of owning equity securities like corporate stock or capital interests in a partnership. Other fancy names for phantom equity include restricted stock units or RSUs, simulated stock, shadow stock, and synthetic equity. There is no single uniformly accepted term, nor is there one commonly used design.

But avoid confusing a phantom unit with actual equity securities denominated in units, e.g., LLC units. An LLC with equity securities called LLC units can grant phantom LLC units.

How does phantom equity work?

Most phantom equity awards are a contractual promise to issue equity securities in the future if certain conditions are satisfied. Satisfaction of these conditions is commonly called vesting.

For example, Apple awards employees both time- and performance-based RSUs. Time-based RSUs vest annually over three years, so long as the employee remains employed on each vesting date. On or shortly after a vesting date, Apple issues the employee shares of Apple stock equal in number to RSUs that vest on that vesting date.

Apple's performance-based RSUs, by contrast, vest if Apple's total shareholder return hits certain targets. Once a target is hit, Apple issues shares equal in number to RSUs associated with that target.

Can private companies award phantom equity?

Yes. Indeed, phantom equity is often used by corporations that need or want to limit the number of their stockholders, e.g., S corporations. Phantom equity is not limited to corporations; partnerships and LLCs can also grant phantom equity. For many private companies, vesting and payment of phantom equity awards are conditioned on a liquidity event like the sale of the company.

What vesting conditions are allowed?

Like Apple's RSUs, most phantom equity vests based on continued employment over time or the achievement of a company or individual performance target. But there is no limit on the vesting conditions that you can devise. You can condition vesting on both service and performance. Vesting can be conditioned upon the sale of the company for a minimum price.

Vesting can also accelerate, fully or partially, upon specified events. The

continued on page 5

continued from page 4

vesting of many phantom equity awards, including Apple's RSUs, typically accelerates upon the award recipient's death or disability while employed. Also common is vesting acceleration upon a change in control of the company, but the trend is toward vesting acceleration upon termination of employment during a specified time (usually, one to two years) after the change in control. You may have heard of the former referred to as "single trigger" and the latter as "double trigger" vesting, morbid as that sounds.

Although it is uncommon, phantom equity can be fully vested when granted. This gives the award recipient a guaranteed right to payment on a future date or upon a specified event like termination of employment or sale of the company. Beware, however, that when vesting and payment do not roughly coincide, different tax withholding is required for each event (see below), and the phantom equity award might be subject to complicated tax rules for deferred compensation. Check with a professional familiar with Section 409A of the federal tax code.

How are phantom equity awards different from actual equity awards?

An actual equity award like restricted stock involves an immediate stock issuance on the grant date. The stock is usually nontransferable and forfeitable until vesting conditions are satisfied. With phantom stock, by contrast, no actual stock is issued on the grant date. Put differently, a recipient of restricted stock immediately becomes a stockholder with voting and dividend rights whereas a recipient of phantom stock does not. This difference has important tax consequences described below.

Does phantom equity have to be paid in securities?

The term "phantom equity" is somewhat of a misnomer because there is no requirement for an award to be payable in equity securities. A phantom award can be payable in cash, gold bullion, or any other property. Cash-settled RSUs, for example, are basically cash bonuses with the payment amount calculated from the value of the underlying stock.

For example, assume that Apple's RSUs are settled in cash instead of shares. On each vesting date, Apple would pay the employee a cash amount equal to the number of vested RSUs times the fair market value per share of Apple stock.

Can phantom awards be granted to directors, consultants, or independent contractors?

Yes, but any payment must be treated as compensation.

How are phantom awards taxed?

The grant of a phantom award usually is not a taxable event because no shares or other property is transferred to the award recipient. When a phantom award vests, an employee is taxed for FICA and FUTA, regardless of when the award is actually paid. When the award is paid, income tax withholding is due for employees. You cannot withhold any taxes for non-employees.

Most phantom awards are paid on or soon after vesting, so FICA, FUTA, and income tax withholding are all due at once. If there is a long delay between vesting and payment, however, tricky rules on deferred compensation might apply so check with tax counsel when designing complicated vesting schedules.

The amount subject to withholding taxes is the current value of the award or payment, i.e., the amount of cash or value of shares or other property payable.

For an employer, the amount paid to the phantom award recipient is deductible as compensation.

How is tax withheld for phantom awards payable in equity securities?

A phantom award recipient's portion of income and employment taxes that an employer must withhold can be paid in a few ways. The easiest way is to collect payments in cash or check or request authorization to withhold from payroll. Another way is called "net settlement" and involves reducing the total number of equity securities to be issued by the number of securities with a value equal to or less than the taxes due.

Public companies have the option of broker-assisted cashless settlement or same-day sale (also called sell-to-cover), i.e., selling a portion of the number of shares to be issued with a value equal to or less than the taxes due. It is rare, but not a problem, for an employer to loan or pay the amount of taxes due from a phantom award recipient.

Each way of paying income and employment taxes presents unique administrative challenges, so plan ahead.

Can a phantom award recipient make an 83(b) election?

You may have heard of an optional election under Section 83(b) of the federal tax code. Ordinarily, the recipient of restricted property (e.g., restricted stock) is taxed when the property becomes transferrable or no longer subject to a substantial risk of forfeiture (e.g., when restricted stock vests). But the recipient can make an 83(b) election and instead be taxed when the restricted property is received (e.g., when restricted stock is granted). This makes sense for recipients of restricted stock in a start-up company with shares that have little or no value on the grant date.

A recipient of a phantom award cannot make an 83(b) election because the election only applies to the transfer of restricted property. Because no property is transferred on the grant date of a phantom award, no 83(b) election can be made. In short, you can make an 83(b) election for restricted stock, but not for restricted stock units.

Are phantom awards right for my company?

Consider phantom awards if you want to link compensation to your company's success, but you are constrained by the number of equity securities you can issue

continued on page 6

continued from page 5

or the timing of when you can issue them. If issuing equity securities as compensation is just too administratively burdensome, phantom awards might be a practical alternative. But do not overlook the benefit of phantom awards because they sound mysterious and complicated when they are not.

Disclaimer: This is for general information and is not intended to be and should not be taken as legal advice for any particular matter. It is not intended to and does not create any attorney-client relationship. The opinions expressed and any legal positions asserted in the article are those of the author and do not necessarily reflect the opinions or positions of Miles & Stockbridge P.C., its other lawyers or ACC.

Paolo Pasicolan, counsel in Miles & Stockbridge's Baltimore office, focuses his practice on executive compensation, employee benefits, and tax and ERISA litigation. On these matters, he has represented buyers, sellers, lenders, borrowers, and underwriters in hundreds of mergers, acquisitions, and financings.

PRO BONO SPOTLIGHT

We are highlighting below three organizations that offer legal pro bono opportunities in our area. You will be seeing representatives of theirs at upcoming luncheons.

PRO BONO RESOURCE CENTER OF MARYLAND

Pro Bono Resource Center of Maryland connects attorneys to meaningful pro bono opportunities based on their substantive interests and geographical preferences. Attorneys can volunteer in many ways across Maryland – from direct representation and giving brief advice at legal clinics to answering calls on a hotline, serving as a volunteer mediator, or assisting with research and writing projects – and training is often available for new volunteers. For information about available opportunities and PBRC's pro bono projects, please visit www.probonomd.org/volunteer. To register for upcoming live trainings or online webcasts, please visit www.probonomd.org/training.

MARYLAND VOLUNTEER LAWYERS SERVICE

Founded in 1981, Maryland Volunteer Lawyers Service (MVLS) provides quality civil legal assistance to Marylanders with limited income at low or no cost. MVLS is the largest pro bono legal services provider in Maryland, both in terms of volunteers, over 1,600 lawyers on its panel, and clients served, 80,000 since 1981. MVLS was created to expand the capacity of Maryland's overburdened legal services delivery system which can serve only 20% of low-income residents who need critical civil legal services. Our core pro bono program matches volunteer lawyers with low-income Marylanders who need civil legal assistance. MVLS also offers a variety of other volunteer opportunities such as legal clinics, mentoring, presenters for our trainings, and presenters for "Know Your Rights" clinics at community-based nonprofits in the greater Baltimore area. Last year, MVLS volunteers and staff helped 5,000 low-income Marylanders. To learn more about MVLS go to our website: https://mvlslaw.org

TAHIRIH JUSTICE CENTER

The Tahirih Justice Center is a mission-driven, national non-profit that protects courageous immigrant women and girls who refuse to be victims of violence. Since 1997, Tahirih has answered more than 22,000 pleas for help from individuals seeking protection from gender-based human rights abuses such as domestic violence, female genital mutilation/cutting, forced marriage, honor crimes, rape, torture, and human trafficking. Tahirih's holistic, client-centered legal services include screening, assessment, counsel and advice, and/or full-scale legal representation. Our staff are experts in the areas of Gender-based asylum; Violence Against Women's Act Petitions; T Visas; U Visas; and Special Immigrant Juvenile Status.

Our clients receive culturally sensitive, trauma-informed legal representation from the start to the finish of a case. To increase the number of women and girls we protect, we rely on help from attorneys in our Pro Bono Network. Together, we maintain a 99% litigation success rate, despite the complex nature of our cases. We accept cases that others have deemed "unwinnable" and proudly pioneer in uncharted areas of the law.

New EEOC Guidance for Employees with Disabilities

By Charles R. Bacharach

The EEOC has issued a new "resource document" entitled "Depression, PTSD, & Other Mental Health Conditions in the Workplace: Your Legal Rights." In a press release issued with the guidance, the EEOC noted that charges of discrimination under the Americans With Disabilities Act ("ADA") based on mental health conditions are on the rise. According to the EEOC, preliminary charge data for 2016 shows that the agency "resolved almost 5,000 charges of discrimination based on mental health conditions." EEOC Chairperson, Jenny R. Yang, stated:

> Employers, job applicants, and employees should know that mental health conditions are no different than physical health conditions under the law. In our recent outreach to veterans who have returned home with service-connected disabilities, we have seen the need to raise awareness about these issues. This resource document aims to clarify the protections that the ADA affords employees.

The EEOC states that the guidance is the latest in a series of Q&A format publications aimed at "providing individuals with medical conditions or work restrictions with user-friendly explanations of their rights, and with information that they can give to a health care provider to explain how to provide appropriate medical documentation, if required." Other publications in the series discuss the rights of employees with HIV infection, and the rights of workers who are pregnant.

The EEOC resource document advises employees that if they have a mental health condition that might affect their performance they may have a legal right to a reasonable accommodation that would help them do their job. Examples of possible accommodations listed by the EEOC include:

- altered break and work schedules (e.g., scheduling work around therapy appointments)
- quiet office space or devices that create a quiet work environment
- changes in supervisory methods (e.g., written instructions from a supervisor who usually does not provide instructions in writing)
- specific shift assignments
- permission to work from home

The resource document further advises employees:

> You can get a reasonable accommodation for any mental health condition that would, if left untreated, "substantially limit" your ability to concentrate, interact with others, communicate, eat, sleep, care for yourself, regulate your thoughts or emotions, or do any other "major life activity." (You don't need to actually stop treatment to get the accommodation.)
>
> Your condition does not need to be permanent or severe to be "substantially limiting." It may qualify by, for example, making activities more difficult, uncomfortable, or time-consuming to perform compared to the way that most people perform them. If your symptoms come and go, what matters is how limiting they would be when the symptoms are present. Mental health conditions like major depression, post-traumatic stress disorder (PTSD), bipolar disorder, schizophrenia, and obsessive compulsive disorder (OCD) should easily qualify, and many others will qualify as well.

Employers need to be vigilant in making sure that supervisors and HR employees are aware of the need to be responsive and engage in the required "interactive process" under the ADA when an employee raises the impact that a mental (or other) disability may be having on the employee's ability to work. The EEOC sets the threshold for triggering the interactive process very low. The resource document makes clear that all an employee has to do to be considered for an accommodation is to ask for one from a supervisor, HR manager or other appropriate employer representative. The employee need not invoke the term "accommodation" or any other special words. All that is necessary for the employee to trigger the interactive process is for the employee to seek a change in work conditions due to a medical condition.

The EEOC notes that an employee who cannot perform all the essential functions of his/her job to "normal standards" and has no paid leave, may "still be entitled to unpaid leave as a reasonable accommodation if that leave will help get you to a point where you can perform those functions." The resource document, however, gives no comfort to employers looking to the EEOC for further guidance on "how much is enough" when it comes to leave as an accommodation.

The resource document also advises that an employee who is permanently unable to perform his job may ask to be reassigned to a job that the employee can do as a reasonable accommodation, if such a position is available.

The EEOC states that an employer may seek information supporting the employee's claimed need for an accommodation from the employee's health care provider. To assist employees, the EEOC supplies a link to a companion document entitled "The Mental Health Provider's Role in a Client's Request for a Reasonable Accommodation at Work." Like the employee resource document, the guidance for health care providers is presented in a Q&A format. A number of the "answers" closely track the employee

continued on page 8

continued from page 7

resource document on the basics of the ADA. Other "answers" are geared specifically to the health care provider's role. For example:

> How Can I Help My Client Get a Reasonable Accommodation?
>
> Your client may ask you to document his or her condition and its associated functional limitations, and to explain how a requested accommodation would help. The employer, perhaps in consultation with a health care professional, will use this information to evaluate whether to provide a reasonable accommodation, and if so which one. The person evaluating the accommodation request also may contact you to ask for clarification of what you have written, or to provide you with additional information to consider. For example, you may be told about a particular job function and asked whether the requested accommodation would help your client to perform it, or you may be asked whether a different accommodation would be effective where, for example, the requested accommodation would be too difficult or costly for the employer to provide.

The guidance to health care providers states that employers cannot take adverse action against their patient based on the information the provider supplies, unless the information shows that the employee is unable to perform the essential duties of the job even with a reasonable accommodation.

Although the Mental Health Providers' document is essentially a "how to" guide for employees and their health care providers, it does provide employers with some guidance as well. The document describes the type of documentation employers may seek from health care providers and may aid employers in seeking information from mental health care providers, who are often reluctant to supply more than a minimum of information concerning their patients. Categories outlined by the EEOC include:

- A brief statement of the health care provider's qualifications and the nature and length of the provider's relationship with the employee/client.
- The general nature of the employee/client's condition, although, not necessarily the specific diagnosis.
- The employee/client's functional limitations absent treatment – although the EEOC states that it is sufficient to show the substantial limitation of just one major life activity.
- An explanation of the employee/client's need for a reasonable accommodation, including the specific problems that might be helped by the accommodation.
- The suggested accommodation(s). The EEOC cautions providers: "Do not overstate the need for a particular accommodation, in case an alternative is necessary."

The EEOC will almost certainly face increased critical scrutiny from the Trump administration. It is unclear, however, to what extent, if at all, that scrutiny might affect this guidance.

Taken together, the two guidance documents reveal the EEOC's belief that employees have broad entitlement to accommodations for mental conditions. Determining how to respond when an employee seeks an accommodation has become one of the most prevalent and difficult issues employers face. The answers often are not clear, and errors in judgment can expose employers to significant liability under the ADA and similar state laws.

For More Information Contact:
Charles R. Bacharach
cbacharach@gfrlaw.com
410-576-4169

Save The Dates!

May 15
Annual GOLF/SPA Event at Elkridge Country Club and About Faces Spa in Kenilworth

May 23--Luncheon sponsored by Whiteford Taylor & Preston

June 8--Welcome Summer Evening Social--Mustang Alley--5:30 to 8:30--sponsored by our premiere sponsor--Womble Carlyle

June 13--Luncheon sponsored by Shawe & Rosenthal

September TBD--Luncheon sponsored by DLA Piper

October 12--Luncheon sponsored by Womble Carlyle

October 15-18--ACC National Annual Meeting in Washington DC

November TBD--Luncheon sponsored by Saul Ewing

Don't Check That Box: The Problem with the new EU Privacy Shield

By Newt Fowler and Ted Claypoole, Womble Carlyle

The EU-US Privacy Shield is a legal framework for exchange of personal data for commercial purposes between the European Union and the United States. In theory its purpose is to enable US companies to receive personal data under the EU laws designed to protect EU citizens. Any US company doing business in the EU which might receive consumer data – no matter how small an enterprise – should be more than curious about how these new EU privacy rules might apply and whether a new "safe harbor" regarding such data is the best solution to the maze of new regulations and compliance risks. A safe harbor sure sounds reasonable enough, doesn't it? The safe harbor is actually where the headache begins for US companies handling EU consumer data.

Amid the dozens of requirements in the newly-passed EU Privacy Shield, sits a seeming innocuous promise that may turn out to be the source of unfathomable fines for US businesses. Unwitting companies that are simply checking boxes to assure compliance with the Privacy Shield may have to change entire business models or face the wrath of European Data Protection Authorities.

Hidden down deep in amongst the redress options and the monitoring mechanisms is a simple statement required of US companies. The Privacy Shield documents require that any business seeking its protection must agree to the core principals of the EU data protection regime, specifically, the principals of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability.

While all of these principals seem on their faces to be vaguely reasonable concepts in holding and transferring personal data – who can argue with Data Integrity or Data Security, for example? – their very vagueness will lure US businesses into must stricter limitations on their own business models, or else risk fines that could run to four percent of worldwide gross revenues. In other words, complying with the Privacy Shield means acceding to the European vision of data as tightly restricted in use and movement without explicit permission from the data subject.

Specifically, many sophisticated US companies, including huge enterprises like Microsoft, Google or Facebook, build files of data and attach those files to the individual that the data describes. Transactional data, like what a person purchases, what account is used, descriptive data like location and specific computers used, and incidental data like search history and browser history are all collected and applied for advertising regimes and innumerable other functions. Many other companies extrapolate secondary or tertiary information from personal data and aggregate those results into useful lists. All of these activities are likely to be unlawful under the Data Shield Principals that US businesses are being asked to accept.

Those companies complying with the Privacy Shield will have not only agreed to "Purpose Limitation" restrictions, but also agreed to "Recourse, Enforcement and Liability" provisions that demand punishment for the company that fails to comply. The Purpose Limitation Principal is defined as "ensuring that personal data is only processed for the purposes for which it was collected, subject to further consent from the data subject." Nowhere does this requirement appear in US law to restrict American businesses from building internal knowledge, or to force those businesses to send a request to all people represented by information in the companies' databases for every new query that the companies might have.

US companies have built their business models in the absence of such restrictions and complying with those restrictions could destroy important sources of customer information and revenue, developed over decades of experimentation. By agreeing to the terms of the Privacy Shield, these important business tools will be at risk and companies using them would be submitting themselves to the scant mercy of the various EU Data Protection Authorities.

In addition, the vague concept of "Purpose Limitation" has never been well-defined or closely understood in the recent history of gathering electronic data. If customer information is collected for the purpose of completing a transaction, then, under a "Purpose Limitation" regime, that data should not be used once the transaction is complete (including, one assumes, delivery of a purchased item). But where a consumer provides a name or other personal data for other reasons, where does the right to use the data stop? From a Data Protection Authority's position, the onus would be on the company receiving information to define its initial use, so the company can ask for permission for further use, but this has never been the way US firms conduct business online. In addition, would the "Purpose Limitation" apply to aggregated use, or extrapolation of secondary information from various databases?

The rule is not clear, but the EU Data Protection Authorities, especially in German states, have demonstrated a willingness to be aggressive in trying to force US businesses into the most restrictive perceived EU rules. We predict this particular aspect of the Data Shield will yield confusion and sanctions for many US companies in the coming years.

Finally, if US companies take the required action to meet EU Privacy Shield requirements, and agree in their publically published privacy policies that those companies support and comply with "Purpose Limitation," among other things, in their treatment of personal data, have they just imposed a restriction on their use of data collected from North America? If so, this would be a restriction that no US legislature or regulatory agency has imposed on collection and use of general personal data. But after making such public assurances, many US companies have subjected themselves to FTC enforcement actions if the companies continue to use personal data in the ways they always have before and now in violation of their own EU modified policies.

continued on page 10

continued from page 9

The FTC can claim that these companies have unfair and deceptive trade practices under the FTC Act for using customer personal information in ways that extend beyond the original purpose of its collection. US executives should think hard about alternatives before blithely making "Purpose Limitation" promises in their privacy policies.

Unfortunately, US companies are entering a brave new world of how to handle and use personal data collected around the globe. There is no easy "check the box" solution for those doing business in the EU and they should not be lulled into the path of least resistance when sorting out how to handle EU consumer data. It is possible that many companies will face having to change their business models regarding data access, use and permission to avoid finding themselves within the line of fire from EU regulators. Doing nothing isn't an option, nor is blithely checking the box.

Newt Fowler leads Womble's Baltimore corporate team. Newt has extensive experience guiding middle market companies through Private Equity/VC financings and M&A transactions, as well as technology and IP transactions. He also Chairs the Maryland Technology Development Corporation (TEDCO).

Newt Fowler
410-545-5871
nfowler@wcsr.com

Ted Claypoole is one of the most respected attorneys in the privacy and data security field and has co-authored two books on privacy and data security with former White House CIO Theresa Payton.

Ted Claypoole
(704) 331-4910
TClaypoole@wcsr.com

Maryland General Assembly Passes Paid Sick and Safe Leave: What Employers Should Know

By Puja Gupta, Jackson Lewis

Maryland may soon be joining seven other states with mandatory paid sick and safe leave following the Maryland General Assembly passage of the Maryland Healthy Working Families Act[1] on April 5, 2017. The Act requires most employers to provide paid sick and safe leave to their employees. The Act has an effective date of January 1, 2018.

As of the date of this writing, Maryland Governor Larry Hogan has not acted on the enrolled bill, although he has promised to veto it.[2] Both the Maryland Senate and the House of Delegates passed the bill by a veto-proof majority. If the Governor vetoes the bill, the legislature may override the veto during next year's legislative session, which could delay the effective date.

1. What does the Act require?

If enacted, the bill would require employers with at least 15 employees to provide up to 40 hours of paid sick and safe leave per year to their employees. Employers with fewer than 15 employees would be required to provide up to 40 hours of unpaid sick and safe leave days to their employees. Paid sick and safe leave must be paid at the same wage rate that the employee normally earns. The number of employees is determined by calculating the average monthly number of employees employed by the employer during the immediately preceding year, without regard to any employee's full-time, part-time, temporary, or seasonal employee status.

a) The bill defines the scope of permissible uses for sick and safe leave broadly.

The most significant impact of the bill for employers with a sick leave benefit already in place will be on the permitted uses for sick and safe leave. Employers are required to permit employees to use sick and safe leave for the following reasons:

- to care for or treat the employee's mental or physical illness, injury, or condition;
- to obtain preventive medical care for the employee or his or her family member;
- to care for a family member with a mental or physical illness, injury, or condition;
- for maternity or paternity leave; or

continued on page 11

continued from page 10

- if the absence from work is necessary due to domestic violence, sexual assault, or stalking committed against the employee or the employee's family member, and
  - » the leave is being used by the employee to obtain for him or herself or his or her family member: (1) medical or mental health attention that is related to the domestic violence, sexual assault, or stalking; (2) services from a victim services organization related to the domestic violence, sexual assault, or stalking; or (3) legal services or proceedings related to or resulting from the domestic violence, sexual assault, or stalking; or
  - » the leave is being used by the employee during the time that the employee has temporarily relocated due to the domestic violence, sexual assault, or stalking.

b) The bill requires an employer to permit employees to accrue sick and safe leave at a specific rate bound by certain limitations.

All employees covered by the bill are entitled to accrue one hour of sick and safe leave for every 30 hours worked. Employees who are exempt under the federal Fair Labor Standards Act are assumed to work 40 hours each week, unless the employee's normal workweek is less than 40 hours, in which case the number of hours in the normal workweek should be used to assess an employee's sick and safe leave accrual.

Employers need not allow an employee to earn more than 40 hours of earned sick and safe leave in a year. Employers need not allow an employee to use more than 64 hours of earned sick and safe leave in a year. And employers need not allow an employee to accrue a total of more than 64 hours of earned sick and safe leave at any time. Employers are not required to permit an employee to use accrued sick and safe leave during the first 106 calendar days that the employee works for the employer.

Although employers are permitted to simply award an employee the full amount of earned sick and safe leave that he or she would earn over the course of a year, rather than awarding sick and safe leave as it accrues during the year, part-time employees may be affected by the general rate of accrual provided by the bill. For example, under the bill, an employer is not required to allow an employee to accrue sick and safe leave during a two-week pay period in which the employee worked fewer than 24 total hours, during a one-week pay period if the employee worked fewer than a combined total of 24 hours in the current and immediately preceding pay periods, or during a pay period in which the employee is paid twice a month (regardless of the number of weeks in a pay period) and the employee worked fewer than 26 hours in the pay period.

c) The bill requires an employee to carry over some portion of a balance of unused earned sick and safe leave from one year to the next.

If an employee has unused earned sick and safe leave at the end of any year, the bill entitles the employee to carry over a balance that need not exceed 40 hours of earned sick and safe leave to the next year. An employer, however, is not required to permit an employee to carry over unused earned sick and safe leave if the employee already has accrued 64 hours of earned sick and safe leave, if the employer awards the employee the full amount of sick and safe leave at the beginning of the year, or if the employee is employed by a nonprofit or governmental unit in accordance with a grant for a non-renewable one-year term.

Additionally, an employer that acquires another employer is required to permit employees of the original employer who remain employed by the successor employer to retain all of their unused earned sick and safe leave accrued during the employees' employment with the original employer.

d) The bill requires the employer to reinstate unused earned sick and safe leave for certain employees.

If an employee is rehired by the employer within 37 weeks after leaving the employment of the employer, the employer must reinstate any unused earned sick and safe leave that the employee had when the employee left that employer's employment. If, however, the employer voluntarily paid out the employee's unused sick and safe leave to that employee upon the termination of his or her employment, the employer need not reinstate the previously unused earned sick and safe leave to the rehired employee.

2. Exceptions to what the Act requires.

The Act does not cover employees who:

- work under a contract for hire;
- are under the age of 18 before the beginning of the year;
- are temporary employees of an employer, or individuals employed by a temporary services agency to provide temporary staffing services—so long as that staffing agency does not have day-to-day control over the work assignments and supervision of the individuals;
- are employed in the agricultural sector or an agricultural operation;[3]
- work fewer than 12 hours a week;
- are employed in the construction industry and are covered by a collective bargaining agreement that expressly waives the requirements of the Act; or
- are called to work on an as-needed basis in a health or human services industry, can reject or accept the shift offered by the employer, are not guaranteed to be called on to work by the employer, and are not employed by a temporary staffing agency.

But the Act provides that janitors, building cleaners, building security officers, concierges, doorpersons, handypersons, and building superintendents do not fall into the category of individuals employed in the construction industry.

With regard to exceptions to the amount of pay for paid sick and safe leave, an employer is not required to pay a tipped employee more than the applicable minimum wage for earned sick and safe leave.

continued on page 12

continued from page 11

3. What right does the employer have to advanced notice or to deny use of leave?

The bill permits employers the right to adopt and enforce a policy that prohibits the improper use of accrued sick and safe leave and prohibits a pattern of abuse of the use of accrued sick and safe leave. Under the proposed Act, employers can require the employee to provide reasonable advance notice of not more than seven days before the date the employee's use of sick and safe leave would begin if the need to use it is foreseeable. But if it is not foreseeable, the employee must provide notice to the employer as soon as practicable and generally comply with the employer's notice or other procedural requirements for requesting or reporting other leave.

An employer can also require an employee who uses earned sick and safe leave to provide verification that the leave was used appropriately if the leave is used for more than two consecutive shifts, or the employee used the leave during the period between the first 107th and 120th calendar days of the employee's employment and the employee agreed to provide verification under terms mutually agreed to by the employer and employee at the time of his or her hiring.

If an employee fails or refuses to provide verification of his or her use of sick and safe leave, the employer can deny a subsequent request to take earned sick or safe leave for the same reason. An employer is permitted to deny a request to take earned sick and safe leave under two additional circumstances. First, an employer can deny the use of sick and safe leave if the employee fails to provide the notice required and the employee's absence will cause disruption to the employer. Second, a private employer licensed to provide services to mentally ill or developmentally disabled individuals can deny use of sick and safe leave if the need to use the earned sick and safe leave is foreseeable; after exercising reasonable efforts the employer is unable to provide a suitable replacement employee; and the employee's absence will cause a disruption of service to one or more individuals with a mental illness or developmental disability.

4. How does the bill affect shift workers?

Employers are not permitted to require employees who request to use sick and safe leave to search for or find an individual to work in his or her place while the employee takes the leave. Generally, only if both the employer and employee agree, the employee can work additional hours or trade shifts with another employee during a pay period, or the following pay period, to make up work hours that the employee took off and for which the employee could have taken earned sick and safe leave. But, an employee is not required to offer or accept an offer to make up hours or to trade shifts. And if an employee works additional hours or trades shifts, the employer cannot deduct the employee's absence from the employee's accrued earned sick and safe leave. The employer, of course, is not required to consent to permit an employee to work additional hours or trade shifts if it would result in the employer being required to pay the employee overtime.

However, tipped employees entitled to paid sick and safe leave in the restaurant industry and who need to take earned sick and safe leave, prefer and are able to work additional hours or trade shifts with another employee in the same pay period or the following pay period, and require their employer to arrange coverage of their shift are subject to certain exceptions. For example, if the employer is contacted to arrange the coverage of a shift, the employer has the discretion to offer the employee a choice of either being paid the minimum wage set by law for the employee's absence, or working an equivalent shift of the same number of hours in the same pay period or the following pay period. Employers in the restaurant industry who do not offer their tipped employees either choice must pay the employee entitled to paid sick and safe leave at the rate of minimum wage set by law.

5. Do employers have other rights under the bill?

The bill does not require employers to payout unused earned sick and safe leave accrued by an employee. An employer may allow an employee to use earned sick and safe leave before the employee accrues the amount he or she needs. An employer who does so may deduct the amount paid to the employee for the earned sick and safe leave from the wages paid to the employee upon the termination of his or her employment if the employee leaves his or her employment before he or she has accrued the amount of earned sick and safe leave actually used, and the employer and employee mutually consented to the deduction in a document signed by the employee.

In addition, an employer need only permit the employee to take earned sick and safe leave in the smallest increment that the employer's payroll system uses to account for absences or use of the employee's work time. Employers, however, may not require employees to take sick and safe leave in an increment greater than four hours.

6. Enforcement provisions include the creation of a civil cause of action and right to receive treble damages.

The bill proposes that employers must provide notice to employees concerning how earned sick and safe leave is accrued, the permitted uses for earned sick and safe leave, and a statement regarding the bill's prohibition against an employer taking adverse action against one who exercises rights under the proposed Act, as well as a statement regarding the bill's prohibition against an employee making a complaint, bringing an action, or testifying in an action in bad faith. If enacted, the Act would create a right for an employee to report an alleged violation of the Act to a Commissioner and to file a civil cause of action for the same. A court (or the Commissioner to whom a complaint is made) may award a prevailing employee three times the value of the employee's unpaid earned sick and safe leave, punitive damages, reasonable counsel fees and other costs, and injunctive relief.

continued on page 13

continued from page 12

7. Conclusions

Under the bill, an employer need not modify its existing paid leave policy if it permits an employee to accrue and use leave at a rate at least equivalent to the sick and safe leave provided by the bill, or the employer's existing leave policy does not reduce an employee's compensation for an absence due to sick or safe leave. Naturally, an employer with at least 15 employees that has a paid leave policy that permits employees to access and accrue paid leave at the same or a greater rate than that provided for in the bill, and permits its employees to use paid leave for any of the purposes provided in the bill, should generally be deemed to have a paid leave policy equivalent to the requirements under the proposed Act. Given the breadth of permissible uses for sick and safe leave, however, most employers that otherwise provide sick leave or paid time off to employees may find that a review of permissible uses for leave under their current policies is, at minimum, in order.

[1]Labor and Employment—Maryland Healthy Working Families Act, Md. Gen. Assembly (HB1 2017) (enrolled bill *available at* http://mgaleg.maryland.gov/2017RS/bills/hb/hb0001E.pdf).

[2]Ovetta Wiggins and Josh Hicks, *Maryland passes sick-leave bill without votes to override likely Hogan veto*, Washington Post, Apr. 5, 2017, available at https://www.washingtonpost.com/local/md-politics/maryland-passes-sick-leave-bill-with-enough-votes-to-override-likely-hogan-veto/2017/04/05/7039e2b2-1a04-11e7-855e-4824bbb5d748_story.html?utm_term=.cfc22917a2f4

[3]An "agricultural operation" is defined as "an operation for the processing of agricultural crops or on-farm production, harvesting, or marketing of any agricultural, horticultural, silvicultural, aquacultural, or apicultural product that has been grown, raised, or cultivated by the farmer." Md. Code Ann., Cts. & Jud. Proc. § 5-403(a).

Targeting a Government Contractor for Acquisition – Things to Consider First

By Bryan Bunting, Whiteford, Taylor & Preston

Observers of federal government procurements are expecting merger and acquisition activity among government contractors to accelerate under the new administration, particularly in the Defense and IT sectors.[1] Acquiring a company participating in federal government contracting presents unique legal issues that a buyer should evaluate from the time it first considers the transaction. These issues can substantially impact every aspect of the deal, including the form of the transaction, the representations and certifications, the scope of the diligence review, valuation, the regulatory burden involved, and whether the emerging entity will succeed. Importantly, these issues could also arise while acquiring a subcontractor to a federal prime contract, as prime contractors often "flowdown" into the subcontract provisions from their prime contract. Corporate counsel should therefore be alert to these issues in any transaction involving a firm operating in the federal procurement arena. This article identifies seven of the most frequently encountered significant legal issues in a deal involving a government contractor.

1. Anti-Assignment Provisions, Novation, and the Form of the Transaction

The first significant issue, while basic, has an outsized impact on the complexity of the deal. Because of government-imposed anti-assignment provisions, structuring a deal as an asset purchase versus a stock purchase will add post-closing obligations that could be largely avoided through a stock purchase. The government's anti-assignment provisions are designed to ensure that the contract is performed by the entity to which it was originally awarded. Accordingly prime contractors may not assign the performance[2] of their contracts. Unlike many commercial arrangements, no exception exists for situations where another entity obtains "all or substantially all" of the contractor's assets. Contractors may assign performance of a contract only by obtaining a written novation agreement from the government. The government is not obligated to approve the novation, and typically will not even consider it until after closing. Consequently, in an asset purchase, the target must formally continue to perform the government contract post-closing. Depending on the work load and diligence of the contracting officials, consideration of a novation request can take weeks or months. In extreme cases, the contracts may expire before the novation is ever considered.

Conversely, federal law expressly provides an exception to the novation requirement for stock purchases, where the entity performing the contract will not change. Furthermore, notifying the government of a name change is far less onerous than requesting a novation. In all, a stock purchase followed by a name change is ordinarily far more streamlined than an asset purchase.

2. Responsibility and Contractor Ethics: Identifying and Disclosing Potential Claims

Most federal contractors are subject to strict business ethics provisions, imposed not just through their contracts, but also through various statutes that provide for civil or even criminal penalties. In recent years, the government has stepped up enforcement of these provisions, particularly the False Claims Act ("FCA").[3] The government's ability to extract large settlements through the FCA was recently reinforced when the Supreme Court ratified the "implied false certification" theory.[4] Under this theory, contractors may be held liable for failing to disclose non-compliance with material terms of their contracts.[5] For example, if a contract requires services to be provided with employees possessing certain credentials or training, but the contractor uses less skilled individuals to provide the services, a court could find that each invoice the contractor submitted for the services constituted a separate implied false certification. In light of the government's increased enforce-

continued on page 14

continued from page 13

ment emphasis, a critical step in the due diligence process is to review the target's business ethics. Usually, this entails a fulsome review of the target's internal code of conduct, and its ability to monitor compliance with the code. Carefully crafted representations and certifications regarding past business practices and potential claims could also protect the buyer.

3. Organizational Conflicts of Interest

The government's Organizational Conflict of Interest ("OCI") rules are based on two "principles": (1) preventing a contractor from serving in conflicting roles that would undermine the contractor's ability to provide unbiased advice to the government; and (2) ensuring that the contractor does not have an unfair advantage in a competition for a new contract. From these two "principles," government contracts tribunals have elucidated three general "types" of OCIs: (a) unequal access to information; (b) biased ground rules; and (c) impaired objectivity.

Based on the parties' prior business activities, a deal could create any of the three types of OCIs. First, for example, in performing its contracts, the target may have had access to confidential information from the buyer's competitors, or to the government's internal plans for a procurement for which the buyer will compete. Second, the target may be helping the government establish specifications for a new product that the buyer seeks to provide, potentially creating a biased ground rules OCI. Third, the target could be fielding an IT system for a government agency, and be in a position to advise the government on IT hardware of the type the buyer produces, potentially creating an impaired objectivity OCI. Indeed, situations like this third example have been the impetus for several large hardware manufacturers recently divesting their IT services divisions.

Notably, finding an OCI is not necessarily fatal to the transaction, as some types of OCIs can be mitigated. For example, an unequal access to information OCI may be mitigated by imposing an "ethical wall" around the employees that received the sensitive information. Identifying "actual" and "potential" OCIs early in the diligence process aids in implementing effective mitigation strategies.

4. Intellectual Property & Data Rights

If the target created any inventions, developed any software, or provided any data pursuant to a government contract, the government likely obtained at least some rights in it. For inventions that were conceived or first reduced to practice in the performance of a government contract, the government will ordinarily be vested with a paid-up, irrevocable license to practice the invention or have the invention practiced on its behalf anywhere in the world. In other words, even though the target may profit from the invention in the commercial sector, it will never again earn anything from federal government for that invention. In some circumstances, the government could even have full title to the invention.

With respect to software and data, the government could possess a wide range of rights. At one end of the spectrum are "Unlimited Rights," which allow the government to use or modify the software or data in any way for any purpose. For data, Unlimited Rights also allow the government to provide the data to third-parties free of charge. At the other end of the spectrum, when the government obtains software as a commercial item, it may do so pursuant to the contractor's standard commercial End User License Agreement. Importantly, software and data provided to the government with less than Unlimited Rights usually must be clearly marked as such, or the government may end up obtaining Unlimited Rights anyway. Appropriately marking data is particularly important for subcontractors, who may be unaware that the government may be obtaining rights to further distribute the data. Accordingly, where the target's IP is a part of its value, the buyer will need to carefully review the ownership of the IP and the conditions under which it was provided to the government.

5. Size Status for Small Businesses

The government offers a variety of socio-economic preferences for small and socially disadvantaged entities seeking to do business with the government. When determining whether the contractor is "small," the government considers either the contractor's number of employees or annual revenue, depending on the industry involved. Importantly, the government considers all of the contractor's "affiliates" when calculating total employees or revenue. Common ownership is one of many ways by which firms can be "affiliated." Accordingly, even in a stock purchase, where the target remains a separate legal entity, its total calculated size will increase to include the buyer's employees and revenue, potentially jeopardizing its size status. While the target could continue to perform any contract that it was previously awarded based on its small size, it would no longer be able to benefit from the socio-economic preferences for new procurements, which could affect its valuation, or even its long-term viability.

6. Cost Issues

If the target holds any cost-reimbursement type contracts, it will be subject to additional, onerous accounting rules and audits that do not apply to government contractors that perform only fixed-price contracts. Specifically, the government's unique "Cost Accounting Standards" apply to most higher-valued cost-type contracts, and require contractors to deploy specialized accounting systems. In addition, the target's entitlement to payment of its costs incurred in performing the contract will be limited to those "allowable" under the Federal Acquisition Regulation. The government will audit the contractor's claimed costs for each fiscal year, and potential "disallow," and thus recoup, costs it previously paid. The government could also impose additional penalties if it deems the costs to be "expressly unallowable." Many government agencies are years behind in performing their annual audits. The

continued on page 16

AUTHORIZED BY JOHN B. FRISCH, CHAIRMAN & CEO

Through the power of diversity and inclusion, the law firm of Miles & Stockbridge delivers richer, better solutions for our clients and communities.

MILES & STOCKBRIDGE

milesstockbridge.com

continued from page 14

target therefore could be subject to a claim for disallowed costs and penalties for years after the closing, based on business activity that occurred years before the closing. The buyer should identify all cost-type contracts during the diligence process and determine the status of their audits. Well drafted representations and certifications, or even an earn-out provision, could further protect the buyer.

7. Special Issues with Foreign Buyers

Finally, there are at least three additional significant issues that may arise in the context of a foreign buyer. First, the government may terminate the target's contracts if it deems the emerging entity to be an "inverted domestic entity," i.e., one that was created for the purposes of avoiding United States tax jurisdiction. Second, if the target holds any classified contracts, the deal will raise Foreign Ownership, Control or Influence (FOCI) concerns that could disrupt the target's ability to continue to perform the classified contracts. Third, as with any deal involving a foreign buyer, the Committee on Foreign Investment in the United States could bar the transaction based on national security concerns, which are necessarily heightened for defense and intelligence contractors.

[1]*See, e.g.,* F. Konel, *Here's Why Defense IT Firms Should Brace for Merger Mania*, Nextgov.com (Jan. 9, 2017), available at: http://www.nextgov.com/defense/2017/01/heres-why-defense-it-firms-should-brace-merger-mania/134440/ (last visited May 2, 2017).

[2]An exception exists for assigning payments due under a contract. The government has provided procedures by which contractors may as a matter of routine assign payments to a third party such as a lender.

[3]31 U.S.C. § 3729(a)(1)(A)

[4]*Universal Health Servs., Inc. v. United States ex. rel. Escobar*, 579 U.S. __, 136 S. Ct. 1989, 1993, 195 L. Ed. 2d 348 (2016)

[5]*Escobar*, 136 S. Ct. at 2001.

Board Leadership