Inside 4Q2019

ACC Association of Corporate Counsel
BALTIMORE

FOCUS

President's Message

Prabir Chakrabarty

Wow, it is very hard to believe that my term has passed this quickly. Given that this is my final message as President, I want to thank everyone for an amazing year! I am so grateful to the Members, the Sponsors, the Board and the best ACC Chapter Administrator bar none, Lynne Durbin, for support of our chapter and attendance at our events. I would also like to personally thank Whitney W. Boles for all of her help with the Newsletter this year.

In line with the other wonderful occasions we have had this year, our Sponsor Social at the Ravens Stadium and the Fall Social at the Guinness Brewery with Nelson Mullins, LLP had great weather, food and drink. Our luncheons were also a great success including Shawe Rosenthal's presentation of the Top 10 Reasons Employees Sue, the joint ACC and MSBA "Coffee with Counsel" with Baltimore City Solicitor Hon. Andre M. Davis, the fantastic panel on Diversity by Womble Bond Dickinson and Saul Ewing's Presentation on Annual Business Checkups and Pressing In-House Business Issues. We also contributed to the Baltimore community through our Pro Bono Senior Estate Planning Clinic at Keswick Multi Service Center in partnership with the Bar Association of Baltimore City Senior Legal Services and the Exelon Pro Bono Program.

I will remain involved with the ACC Baltimore Chapter, but I also hope to be a more active member of the ACC Financial Services Network and I urge all ACC members to join a network as they offer the ability to quickly access relevant, industry-specific resources to help you impact your profession. As this goes to press we will have finished the ACC Annual Meeting in Phoenix, Arizona. I encourage every ACC member to attend the Annual Meeting, which is an incredible conference that gives you the opportunity to meet thousands of other in-house counsel from around the world.

It has been a pleasure serving this Chapter and I look forward to interacting with everyone in the future!

Best Regards,
President
Prabir Chakrabarty

Upcoming Events

December 10
Lunch with Anderson Kill on Big Data.

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

Prabir Chakrabarty —President

Board Members:

Larry Venturelli
President elect and Treasurer

Dan Smith— Secretary

Cory Blumberg

Whitney Boles

Taren Butcher

Dee Drummond

Joseph Howard

Raissa Kirk

Kimberly Neal

Noreen O'Neil

Danielle Noe

Michael Wentworth

Matthew Wingerter

Karen Davidson
Immediate Past President

Template for Disaster

By Neil Peretz

"Who knows what evil lurks in the hearts of agreements?" Not you, if you have an over-reliance on templates.

As a former litigator, I have witnessed numerous scenarios where a slavish devotion to template agreements paved the road to disaster. Organizations felt that the template agreement was sacrosanct and dared not contemplate how new facts and situations might require its alteration.

Obeisance to and reliance upon a "template" is not surprising, given the history of the term. The etymology of "template" traces back to the Latin word "*templum*," which means not only "plank or rafter," but also means a "temple, shrine, sacred, or consecrated place."

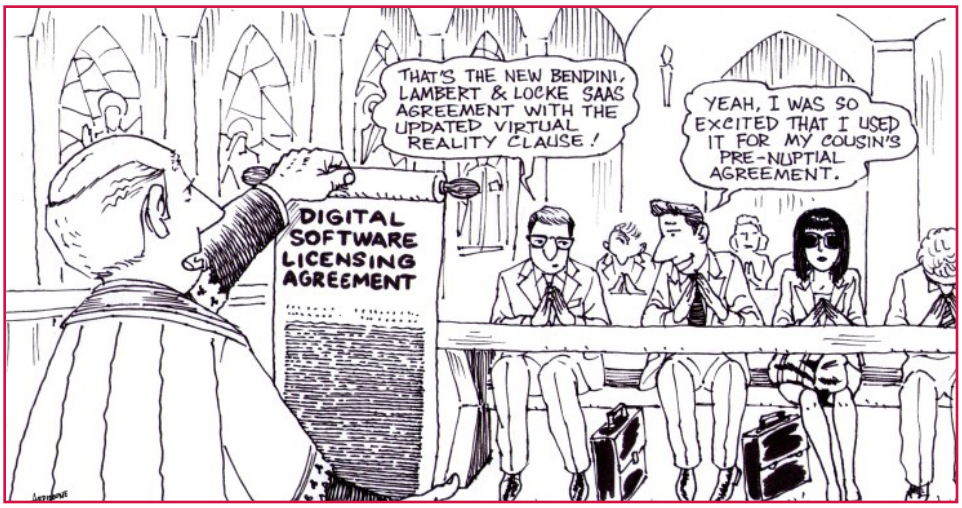
Many cultures have adapted historic religious concepts to today's mores and practices. For example, in most locales, it is no longer de rigeur to stone people to death for working on the Sabbath. (Indeed, there would be much stoning of lawyers if such a rule were still in place.) Similarly, one cannot rely solely on historic templates as the times change.

When translated into Swedish, one word for "template" is "mönster." Remove the diacritical marks above the "ö" and you have the perfect English-language descriptor of templates run amuck.

As a former federal trial attorney and financial services regulator, I often encountered situations where companies violated their own agreements with customers. Why? Because they did not know what was in those agreements.

Maybe once upon a time, they read a template customer agreement but never noted when the template changed — or how each version of their template impacted their practices with respect to future customers. Only after class action or regulatory enforcement did they realize that not all customer agreements were the same.

Using templates lulled them into a false complacency around knowing the



content of their customer agreements. In reality, their templates evolved over time, and they should have been reading and implementing each agreement independently.

In the business-to-business context, an over-reliance on templates can lead to even bigger disasters. Businesses are more likely to have attorneys representing them, and business deals are often a higher dollar amount, which means the salespeople pushing the deals are more willing to negotiate in order to get the deal done.

The result is a contract that might look a lot like the standard template agreement yet contains multiple significant deviations from the template that are overlooked during contract implementation … until it's too late.

For example, a major commercial property manager thought its standard lease template was in place with a tenant. The property manager failed to note that the notice requirements had been renegotiated, and, as a result, missed the opportunity to exercise an option to re-assess and potentially raise the rent.

Many large organizations have grown through acquisition. As a result, even if they deploy their own templated agreements going forward, their day-to-day work relies on implementing agreements created by their predecessors and acquisitions. Even if all these inherited prior agreements could be changed, the next acquisition just brings in more types of templates.

Large companies may have hundreds of different agreement templates, meaning they need to start reading each agreement, rather than assuming that all agreements of a certain type are the same. The failure to treat each agreement individually can lead to dangerous assumptions.

For example, some inherited templates might not request that the customer opt-in to receive calls via an auto dialer. The company may face substantial Telephone Consumer Protection Act liability when contacting customers subject to these inherited agreements.

Without careful attention to the contents of each agreement, the use of templates can breed a pernicious complacency throughout the organization. Employees assume that agreements need not be read because they are inviolable and blessed from above.

When a new situation arises where the standard template doesn't fit, the employee chooses to use the template regardless, because doing so creates the least internal organizational friction. The end result is an agreement that doesn't fit the transaction and cannot be smoothly implemented.

continued on page 3

continued from page 2

Surely templates can serve a certain purpose: We cannot afford to write each business agreement from scratch. However, we need to remember that speed in drafting is not the sole benchmark for a successful agreement or successful relationship.

The most successful business relationships are those where both sides receive the benefit of their bargain. This means they need a contract that actually reflects their bargain. And, more importantly, the real relationship work begins after the contract is signed.

Because templates change over time and key terms may be custom-negotiated, implementation of the contract must be based on reading its actual terms, rather than assuming it follows the same format and terms of a mythical template from the past.

As an in-house counsel, you should not assume that the use of a template for a certain type of agreement means that you know the terms of all of your relationships. Start sampling your historic agreements to see how they have changed over time.

If your organization has had acquisitions, sample the agreements of acquired entities as well. And start talking with your business colleagues about how often they need to change agreement terms to conclude a negotiation.

Most importantly, even if you think it's just a standard template that you know by heart, read the key terms of each agreement anyway, because that is what the court and your counterparty will rely upon.

Author:

Neil Peretz has served as general counsel of multiple companies, as well as a corporate CEO, CFO, and COO. Outside of the corporate sphere, he co-founded the Office of Enforcement of the Consumer Financial Protection Bureau and practiced law with the US Department of Justice and the Securities and Exchange Commission. Peretz holds a JD from the University of California, Los Angeles (UCLA) School of Law, an LLM (master of laws) from Katholieke Universiteit Leuven (where he was a Fulbright Scholar), bachelor's and master's degrees from Tufts University, and has been ABD at the George Mason University School of Public Policy. Peretz's most recent technology endeavor is serving as general counsel to Contract Wrangler, which applies attorney-trained artificial intelligence to identify the key business terms in a wide variety of contracts.

ACC News

ACC Xchange: Program Schedule Now Available

Xchange 2020 (April 19-21, Chicago, IL) offers **advanced, practical, interactive, member-driven** education for in-house counsel and legal operations professionals that you won't find at any other conference. By uniting complementary professions to exchange ideas and best practices, this program creates a powerful and unique environment that offers a fresh take on how to deliver your in-house legal services more efficiently and effectively. Register today.

Are your vendors putting you at RISK under the pending California Consumer Privacy Act (CCPA)?

At the ACC Annual Meeting register for, Untangling Third-Party Data Privacy Privacy & Cybersecurity Risk, and learn how to ensure you're ready for the CCPA and your third-party vendors aren't putting you at risk. Save your spot at this session now. Seating is limited.

In-house Counsel Certified (ICC) Designation

The ACC In-house Counsel Certification Program, helps in-house counsel become proficient in the essential skills identified as critical to an in-house legal career. The program includes live instruction, hands-on experience, and a final assessment. Those who successfully complete the program will earn the elite ICC credential. Your law department and your employer will benefit from having a lawyer that returns with global best practices in providing effective and efficient legal counsel. Attend one of these upcoming programs:

- **Dubai, UAE**, March 2-5, 2020

ACC's Top 10 30-Somethings nominations are now open!

This award recognizes in-house counsel trailblazers for their innovation, global perspectives, proactive practice, advocacy efforts, and pro bono and community service work. Self-nominating is acceptable. Nominations are due December 6. Nominate someone today.

Houston, we have a breach. Now what? Lessons learned from the SEC's Facebook settlement

By Sanjay M. Shirodkar, Partner, DLA Piper

In late July 2019, Facebook Inc. entered into a settlement with the Securities and Exchange Commission (the SEC) for making misleading disclosures regarding the risk of misuse of its user data. The SEC asserted that the company had discovered the misuse in 2015, but failed to correct its existing risk factor disclosure for more than two years. Instead, the company's risk factors informed investors that "our users' data may be improperly accessed, used or disclosed" (emphasis added). The company disclosed the incident, but not until March 2018, leading to a large drop in its stock price. The company agreed to pay $100 million to settle the SEC's charges.[1]

Public companies and the general public are becoming increasingly aware of the fact that some sort of cybersecurity breach is being disclosed on a weekly and even daily basis. Much has been written about preventing breaches. But what should companies think about doing when they become aware of a breach? What are some of the lessons learned from the SEC's guidance on this topic, and from the Facebook proceedings? This article explores these topics.

Prior SEC guidance

Here is a brief summary of the relevant SEC and staff guidance:

- CF Disclosure Guidance: Topic No. 2, Cybersecurity, Division of Corporation Finance (October 13, 2011) – the staff of the Division of Corporation Finance provided guidance on how a company could address cybersecurity from a disclosure point of view.[2] The staff guidance reminded issuers to view cybersecurity as a business risk that, like other risks, might require disclosure if it could materially impact a company's operations.
- Commission Statement and Guidance on Public Company Cybersecurity Disclosures (February 26, 2018) – the SEC issued interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. This guidance reminds companies that they should consider cybersecurity risks and incidents when preparing documents that they file with the SEC as the federal securities laws require them to disclose information about material cybersecurity risks and incidents. For example, disclosure may be required in the context of a public company's existing reporting obligations, such as the company's risk factors, management's discussion and analysis, or financial statements. This guidance emphasized the importance of maintaining comprehensive policies and procedures – including effective disclosure controls and procedures – that address cybersecurity risks and incidents. The guidance also noted that company insiders that trade securities while in possession of non-public information about cybersecurity incidents may violate the federal securities laws.[3]
- Securities and Exchange Commission Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 (October 16, 2018) – the staff of the Division of Enforcement and Division of Corporation Finance issued a report pursuant to Section 21(a) of the Exchange Act to make issuers and other market participants aware of certain cyber-related threats and emphasized the need for issuers to consider these threats in devising and maintaining a system of internal accounting controls as required by the federal securities laws.[4]

Lessons learned on disclosure controls and procedures

As we head into the last stages of summer, here are some of the lessons we have learned from the SEC guidance on cybersecurity and the Facebook proceedings that board members and senior management of a public company should consider:

Action item: Review risk factors and other public disclosures. Confirm the accuracy of any disclosures, including risks factors posed as hypotheticals. In the Facebook proceeding, the SEC noted that hypothetical phrasing can create the impression that the episode in question has not occurred. The SEC has previously indicated its view that "it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."[5]

Action item: If you have a policy on a particular topic, ensure that you have a mechanism to summarize or report material violations of the policy to the proper party responsible for ensuring the accuracy of the company' filings with the SEC. According the SEC, Facebook had a set of rules governing what developers are allowed to do with the apps they create

continued on page 5

[1]See, SEC press release dated July 24, 2019 - Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data (available here) and the related complaint (available here). For additional details about this proceeding, see our alert about the parallel FTC complaint and stipulated consent order here. The scope and magnitude of FTC settlement is likely to mean a more aggressive stance by the agency when it comes to enforcing its privacy and data security regime.

This article only discusses the disclosure obligations of a company with respect to the U.S. federal securities laws.

[2]CF Disclosure Guidance: Topic No. 2, Cybersecurity, Division of Corporation Finance (Oct. 13, 2011), available here.

[3]Commission Statement and Guidance on Public Company Cybersecurity Disclosures (February 26, 2018), available here(the SEC Guidance).

[4]Securities and Exchange Commission Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 (October 16, 2018), available here (the SEC Report).

[5]SEC Guidance on page 4.

continued from page 4

and the user data they gathered. However, the company did not have a "specific mechanism to summarize or report" violations of these rules to employees responsible for ensuring the accuracy of its SEC filings.

Action item: Review existing disclosure controls and procedures. Confirm that they are designed to "enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."[6] Ask whether these procedures will "appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings."[7] The SEC observed that Facebook did not "maintain disclosure controls and procedures designed to analyze or assess incidents involving misuse of user data for potential disclosure in the company's periodic reports."

Action item: If an incident has occurred, should a summary of the incident be shared and discussed with outside disclosure counsel and the company's independent auditors in order to assess the company's disclosure obligations? The SEC indicated that Facebook failed to share information about the incident with its independent auditors and outside disclosure counsel in order to assess the company's disclosure obligations.

Action item: Review existing internal accounting controls to confirm that they provide reasonable "assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization."[8] As part of its investigation into several investigations where certain public issuers were the victims of cyber-related fraud, the SEC Report notes that "internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. Public issuers …. must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly."[9]

As part of the FTC proceedings, Facebook agreed to pay a record $5 billion penalty; as part of the SEC proceedings, it agreed to pay a $100 million penalty. These are extraordinarily large fines and may signal the willingness of these agencies to aggressively pursue companies deemed to violate either privacy and data security requirements within the enforcement authority of the FTC or the US federal securities laws overseen by the SEC. With summer winding down, perhaps it is time to look closely at your securities law disclosure. Think about some of the lessons learned. And ask questions.

For more information about the matters discussed in this article, please contact the author or our privacy group at privacygroup@dlapiper.com with questions about privacy and data security matters.

[6] SEC Guidance at page 20.

[7] Id.

[8] SEC Report at page 2.

[9] SEC Report at page 6

Avoid Buyer's Remorse Over EPLI Coverage

By Kirsten M. Eriksson, Principal, Miles & Stockbridge

It has become an unfortunate fact of life that employers get sued by their employees, former employees, and even their independent contractors. To protect against these types of losses, many employers purchase Employment Practices Liability Insurance (EPLI). However, employers who do not carefully read their policies could be surprised by what is (or is not) covered by those policies. They may also be surprised to learn that they cannot use their preferred employment counsel to defend them against these claims. This article provides some tips for evaluating coverage so that employers do not end up with buyer's remorse when they realize they didn't get what they thought they were getting.

EPLI is a relatively new product in the insurance market. It was virtually non-existent twenty-five years ago, and even ten years ago many companies didn't purchase it. These days, having EPLI coverage is very common, but many employers still don't understand the different coverage that is available. EPLI policies can vary in what they cover, and employers should read the coverage provisions closely to make sure that they are receiving coverage for claims that are important to them. Most policies will cover a broad range of claims, such as claims of discrimination, sexual harassment, and wrongful termination. Some, but not all, provide coverage for breach of employment contracts, and defamation or other workplace torts.

Claims that are often excluded include claims under the National Labor Relations Act (NLRA), Occupational Safety and Health Administration (OSHA) claims, and claims of intentional torts. In addition, coverage is often excluded or very tightly constrained for wage and hour claims, such as those arising under the Fair Labor Standards Act (FLSA) and parallel state statutes for overtime and minimum wage violations, with some paying only defense costs (after the deductible is exhausted).

Employers should also understand the dynamics relating to choice of counsel under EPLI policies. Some policies specifically provide that defense counsel

continued on page 6

continued from page 5

will be selected by the insurance company. Others state that the employer may retain qualified counsel of its choosing. Understanding the difference between these clauses is very important. Employers would generally prefer to use their regular employment counsel, who is often someone who has represented the company for years and who knows the company's business, culture, and people. In many cases, the only way the employer will be able to use its preferred counsel is if the policy specifically provides it with the right to select its own counsel. If an employer's policy provides that defense counsel is to be selected by the insurance company, the insurance company may insist that panel counsel a "captive" law firm be used; these firms are engaged by the insurance company in all or most of their matters. The insurers often have negotiated significant rate discounts in exchange for volume. These rates are often far below the lodestar rates the courts use for awarding fees to experienced employment counsel. The quality of work may suffer as well - panel counsel may address the low fees by directing the bulk of the work to inexperienced and often-rotating junior associates.

Even with a policy that gives the insurance company the right to select counsel, a few insurers may be willing to allow employers to use their preferred counsel under certain conditions, particularly if the employer is willing to pay the difference between the insurance panel rate and the counsel's regular rate (although the insurance company often uses only panel counsel's rate in calculating the exhaustion of the deductible). However, many insurers refuse such arrangements and insist upon the use of panel counsel regardless of employer's willingness to pay any difference in rates.

In addition, there can also be a potential for conflicting loyalty when panel counsel is used – since panel counsel's stream of work comes from the insurance company, there may be a temptation to favor the insurance company's interest over the interest of the employer. Indeed, a recent case was filed in California by an employer alleging malpractice against panel counsel and bad faith against the insurance company. The plaintiff-employer claimed that panel counsel "consistently treated Admiral [Insurance Co.] as the 'real' client – consistently favoring Admiral's interests while simultaneously ignoring its responsibilities to [the insured employer]." Specifically, the employer alleged that panel counsel directed the defense of the case toward wage and hour claims that had strict liability limits and away from claims with more expansive coverage.

Finally, employers should be aware of the possible divergence of interest when it comes to settlement of claims. Insurance companies are generally focused purely on the financial implications of a settlement, while employers will often be interested in reputational risk and the risk of being perceived as an "easy target" for employees considering claims in the future. Further, because defense costs generally are included within the limits of liability provided by the policy, an insurance company may not want to pay a high settlement early in the case, hoping that the demand will reduce as the litigation proceeds. However, as defense costs erode the total limits available for settlement, there may not be enough proceeds from insurance to fund a settlement later in the case. There is a potential for even greater conflicts when the insurance provides the cost of defense but not coverage for indemnity, as can be the case in wage and hour claims. In such cases, the goal of resolving the matter on favorable terms can be incompatible with keeping defense costs down for the insurer. This is not to say that all insurance companies or panel counsel are unmindful of their ethical duties to the employer-client. However, this scenario creates a potential for conflict that employers should not overlook.

So, what should an employer do to avoid buyer's remorse? The best time to investigate and negotiate policy language is at the inception of the policy or at renewal, when an employer has its best leverage to negotiate. Employers should take the following steps:

- Don't assume that EPLI is necessary. Employers should analyze the history of their claims and the amounts they have historically spent on defense, and determine whether the cost of coverage, taking into account its limitations and deductibles, is better than remaining self-insured. Some other types of policies (such as directors' and officers' liability policies) may offer endorsements to provide some coverage at a lower cost.
- If coverage makes sense, be sure that the policy includes the types of claims the employer is most likely to face.
- Evaluate how important it is for the employer to be able to use its own counsel. Regular counsel knows the employer and its business – employers won't need to spend significant time explaining the business, history or culture, and regular counsel knows the company's priorities. If choice of counsel is important, be sure to negotiate policy language that permits the employer to select its own counsel and consider agreeing upon hourly rates at the front end.
- Review the clauses in the policy related to settlement. Make sure to understand who gets to decide whether or not to settle, and what are the consequences for the employer if there is a difference of opinion between the insurance company and the employer is there is a difference of opinion about whether or not to settle.
- Understand which claims the insurance company has the obligation to provide an indemnity for, and which it only has the obligation to defend.
- Understand the deductible and limits on liability. Employers should review what defense costs will be applied toward the deductible and whether they will erode the limits of liability to pay any judgment.
- Make sure we've covered all the issues we raised in the article.

continued on page 7

continued from page 6

Employers who understand what an EPLI policy can offer and thoughtfully review the consequences associated with their various choices are much less likely to end up with buyer's remorse.

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, its other lawyers or the Association of Corporate Counsel.

Kirsten M. Eriksson is a principal in Miles & Stockbridge's Baltimore office who co-leads the firm's Labor, Employment, Benefits & Immigration Practice Group. She represents management in all aspects of labor and employment law throughout the country.

Avoiding Jury Trials

By Elizabeth Torphy-Donzella, Alex I. Castelli and Fiona W. Ong, Shawe Rosenthal, LLP

Employers know that juries are fickle and may decide an issue based on empathy and anger rather than the rules of law enunciated in the jury instructions. Thus, there may be a strong interest in avoiding jury trials – but what is the best way to accomplish that? There are several procedural options available to employers – arbitration and jury trial waivers.

The Federal Arbitration Act ("FAA") (and the law of virtually all States that have enacted a version of the Uniform Arbitration Act) enable and support the ability of employers to require arbitration. Contractual agreements that clearly and unmistakably set forth an intent to arbitrate disputes normally will be enforced. The key benefit in arbitration is that there is no jury.

Below are some requirements that must be satisfied in any arbitration agreement to ensure that your employment disputes will be decided by an arbitrator.

- Make sure to identify the disputes that will be subject to arbitration. In all likelihood, you will want to have most everything decided in that forum, including the threshold question of whether a dispute is subject to arbitration. However, if you have restrictive covenants, you likely will want to exclude them from arbitration so that you are not foreclosed from seeking a preliminary injunction in court to stop former employees from using your trade secrets and stealing your customers. Arbitration does not normally provide that relief.
- Know what "consideration" is required in your jurisdiction to create a binding agreement. Consideration is something of value that is given in exchange for a promise. Without consideration, there is no basis for an enforceable agreement. In many jurisdictions, continued employment is consideration for an agreement, but in some, it is not. In those jurisdictions, you will need to provide something more – such as an increase in compensation or a promotion – to create an enforceable agreement.
- Make the duty to arbitrate mutual, and do not include a clause in the agreement that permits the employer to modify or eliminate the agreement to arbitrate at any time for any reason. While this reservation of rights is something that you want to include in handbooks, if you include this clause in your arbitration agreement, you have an illusory promise that will be unenforceable in most States.
- With regard to handbooks, understand that if your handbook is properly drafted, it will have contract disclaimers in more than one place. If your arbitration obligation is contained in the handbook, it will, by definition, be unenforceable because you disclaimed that anything contained in the handbook was contractually binding. That applies to other things like confidentiality requirements – which, in a handbook, may establish policy violations but may not be relied on in court to prove violations of binding duties.
- Make sure that the employer is required to pay the "lion's share" of the fees to arbitrate and that the full panoply of remedies may be obtained by the employee in arbitration. Otherwise, there may be defenses to requiring arbitration of employment disputes.
- Finally, think before you implement. Will you apply this obligation to new hires only, or do you want to try to get signatures from all employees? If the latter, are you willing to terminate employees who refuse to sign?

The use of arbitration agreements is not without some concerns, however. Of note, the #MeToo movement has caused some State legislatures to bar arbitration of sexual harassment claims, thereby complicating the use of arbitration agreements. In 2018, Maryland enacted a law stating:

Except as prohibited by federal law, a provision in an employment contract, policy, or agreement that waives any substantive or procedural right or remedy to a claim that accrues in the future of sexual harassment or retaliation for reporting or asserting a right or remedy based on sexual harassment is null and void as being against the public policy of the State.

See Md. Code Ann., Lab. & Empl. § 3-715(a). Notably, in our work with the Maryland Chamber of Commerce on

continued on page 8

continued from page 7

this bill before it became law, we were assured by the proponents of the bill that it was not intended to bar arbitration of sexual harassment claims. Specifically, the language "Except as prohibited by federal law," was supposed to be the carve-out for purposes of the FAA. But as the language actually reads, it suggests that mandatory arbitration agreements are prohibited.

Yet, even if Maryland's law were deemed to prohibit all arbitration of sexual harassment claims, there is an argument that this prohibition would nonetheless be preempted by the FAA. Recently, a Federal district court in New York compelled arbitration of a terminated employee's sexual harassment claim, despite a similar recently enacted New York law rendering "null and void" any clause in an employment agreement that required an employee to arbitrate sexual harassment claims. *See Latif v. Morgan Stanley & Co., LLC*, 2019 WL 2610985 (S.D.N.Y. June 26, 2019). The court found that application of the State law to invalidate the parties' arbitration agreement would be inconsistent with the FAA. It is likely that other States' bans on arbitration of sexual harassment claims – including Maryland's – will be subject to the same argument, but we will have to wait for litigation in those States on that issue.

Also, be aware that arbitration can be quite expensive. In addition to the initial filing fee, which often is determined by the fanciful damages claim a plaintiff puts in his/her complaint, arbitrators frequently charge at least $450 an hour and often more. They rarely grant a wholesale dismissal without a hearing (a cynical person would say the financial incentive points in the opposite direction) and if you want a written decision at the end, that requires additional time and therefore cost, as will conferences to resolve any disputes during the arbitration process. In addition, discovery often is permitted nearly to the same degree as in court. Thus, contrary to popular perception of arbitration as expedient and low-cost, arbitration normally comes with a hefty price tag and may take almost as long as traditional court proceedings.

If avoiding a jury is a compelling concern for an employer, then another option, if your State permits it, is to have employees sign written agreements that any disputes will be decided by a court sitting without a jury.

The right to a jury trial in civil actions in federal court is guaranteed by the Seventh Amendment of the U.S. Constitution. The Seventh Amendment does not apply to State civil cases, and the right to a jury trial in any State court action depends on the law of the particular State. *See Walker v. Sauvinet*, 92 U.S. 90, 92 (1875). Specifically in Maryland, Article 23 of the Maryland Declaration of Rights guarantees the right to a jury trial in civil cases in Maryland State courts. In *Walther v. Sovereign Bank*, 386 Md. 412, 442 (2005), however, the Maryland Court of Appeals held that parties may contractually waive their right to a jury trial so long as the waiver is "knowing and intelligent."

In *Leasing Serv. Corp. v. Crane*, 804 F.2d 828, 832-33 (4th Cir. 1986), a decision addressing the enforceability of a pre-dispute jury trial waiver, the U.S. Court of Appeals for the Fourth Circuit held that a waiver of the right to a jury trial is valid so long as it is done "knowingly and intentionally" and is "voluntary and informed." In concluding that the waiver at issue was enforceable, the court examined (1) the placement of the waiver in the contract; (2) the circumstances of the parties to the contract; (3) the business acumen of the waiving party; and (4) whether the waiving party had actual knowledge of the terms of the waiver.

Thus, when drafting a jury trial waiver, it is critical to ensure the provision is conspicuous. We recommend the following actions, which have been found sufficient by Maryland courts:

- The provision is clearly titled "JURY TRIAL WAIVER." In this way, there is no confusion about what the purpose of the paragraph is.
- If the jury trial waiver is part of a larger employment agreement, it is set out in its own paragraph, and therefore distinguishable and separate from other provisions. It should not be "buried" amongst many other words dealing with other topics.
- In order to make it stand out and to emphasize its importance, the paragraph should be in all caps and in boldface or a larger font size. This way, employees cannot possibly argue that they overlooked the waiver and did not realize that they were giving up the fundamental right to a jury trial.
- Like an arbitration agreement and for the reasons explained above, it should not be contained in a handbook.
- Just as with arbitration agreements, there must be consideration to make the promise enforceable. Requiring employees to sign at the start of employment, as a condition of employment, when new hires are most willing to sign documents, is optimal.

Whether an arbitration agreement or a jury trial waiver is the appropriate approach will vary from company to company. But both are effective means for employers to avoid jury trials.

Elizabeth Torphy-Donzella and Fiona W. Ong are partners and Alex I. Castelli is an associate at Shawe Rosenthal, a management-side labor and employment law firm based in Baltimore, Maryland. We may be reached at shawe@shawe.com or 410-752-1040.

Elizabeth Torphy-Donzella

Fiona W. Ong

Saul Ewing Arnstein & Lehr Alert

By April F. Doss, Alexander R. Bilus, Patrick M. Hromisin and Jillian K. Walton, Saul Ewing

CCPA Amendments and Draft Regulations Provide Some Clarity, Some Uncertainty, and Numerous Compliance Obligations

Last year, the California legislature passed the sweeping California Consumer Privacy Act of 2018 (CCPA), a far-reaching privacy law that will impact business across the country. Now, in advance of the CCPA becoming effective on January 1, 2020, California's state lawmakers and Attorney General have weighed in with amendments and draft regulations to the CCPA that will substantially impact the steps businesses must take to become CCPA-compliant. This alert discusses: 1) a summary of the CCPA's scope and key provisions, 2) a timeline of key dates and next steps for the CCPA compliance; 3) a summary of the amendments; and 4) an overview of the draft regulations, so that companies can assess how they should proceed in light of these developments.

CCPA Summary and Scope

We have previously written about the CCPA here. The CCPA applies to for-profit entities that collect California residents' personal information, do business in California—even if they are not located in California—and:

- have annual gross revenue exceeding $25 million; OR
- sell or share for commercial purposes the personal information of 50,000 or more California residents, households, or devices; OR
- derive 50 percent or more of their annual revenue from selling the personal information of California residents.

The CCPA may apply to a nonprofit if the nonprofit controls or is controlled by a business that is subject to CCPA and shares common branding with that business.

The CCPA's rights and obligations center around a broad range of personal data, which the law defines as data that relates to individual consumers or households, and which specifically includes:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including online shopping and purchases;
- Biometric information;
- Internet activity;
- Location data;
- "Audio, electronic, visual, thermal, olfactory, or similar information";
- Education and employment information; and
- "Inferences" that are drawn from personal data to create a consumer profile "reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

The CCPA also provides new rights to consumers, including:

- the **right to know** what personal information about them is collected, used, shared or sold,
- the **right to delete** personal information held by businesses,
- the **right to opt-out** of the sale of personal information, with more stringent opt-in and parental consent requirements for the sale of children under the age of 16 and 13, and
- the **right to non-discrimination** in terms of price or service when a consumer exercises a privacy right under CCPA.

And the CCPA imposes new obligations on businesses, including the obligations to:

- **Provide notice** to consumers before or at the time of data collection,
- **Create** procedures to respond to requests from consumers to opt-out, know, and delete information,
- **Respond** to requests from consumers to know, delete, and opt-out within specific timeframes,
- **Verify** the identity of consumers who make requests to know and to delete, and
- **Disclose** financial incentives for retention or sale of personal data.

Key Dates for CCPA Compliance

Although the legislature's amendments have been signed into law and thus are in their final form, the Attorney General's draft regulations are subject to a period of notice and comment before becoming final. As a result, there are still open questions as to what businesses' final obligations will be.

The key dates to note for CCPA compliance are the following:

- From December 2 through 5, 2019, the Attorney General will hold public hearings to solicit comments on the draft regulations in four cities throughout the state.
- December 6, 2019 is the deadline to submit written comments on the proposed regulations.
- On January 1, 2020, the CCPA, as amended, goes into effect.
- The draft regulations are expected to be finalized in the spring of 2020.
- Starting on July 1, 2020, the Attorney General's office will be empowered to enforce the provisions of the CCPA. In his press conference on October 10, the Attorney General indicated that his office will seek to penalize violations of the CCPA that occur between January 1, 2020 and July 1, 2020.
- On January 21, 2021, one-year exemptions relating to employee data and business-to-business data (discussed below) will expire. At that time, unless there are legislative develop-

continued on page 10

continued from page 9

ments within the next year, businesses will be required to fully comply with the CCPA for information collected from employees, job candidates, and between businesses.

Businesses that are subject to the CCPA therefore have to be prepared to comply with the law starting on January 1, but must also be ready to comply with the Attorney General's regulations when they become effective.

The Amendments to the CCPA

Despite intense lobbying efforts during the legislative session, the CCPA's core consumer protections and corresponding obligations on businesses remain relatively unchanged by California lawmakers. Below is a summary of the relevant amendments, which were passed as separate bills by the state Assembly.

One-year delay in effective date for certain employee, job applicant, and business-to-business information—but companies must still beware of breaches: Assembly Bills 25 and 1355 provide businesses with a one-year reprieve (until January 1, 2021) before they must implement CCPA compliance for employee and job applicant data, and for business-to-business communications and transactions. With respect to employee and job applicants, businesses still must inform individuals of the categories of personal information the businesses will collect from employees or job applicants and the purpose for which the information will be used. During this one-year moratorium, consumers, including job applicants and employees, will be able to sue, and employers may face liability to employees and/or job applicants as a result of a security breach of their non-encrypted or non-redacted personal information. With respect to business-to-business communications and transactions, during the one-year moratorium, businesses-to-business consumers have a private right of action for security breach incidents of non-encrypted or non-redacted personal information and the right to opt-out of the sale of personal information.

Slight narrowing of the definition of "personal information": Assembly Bill 874 narrows the definition of "personal information" somewhat by restricting it to information that is "reasonably capable of being associated with, or could reasonably be linked" to a particular consumer or household. This amendment also clarifies that personal information does not include de-identified or aggregate consumer information, and defines "publicly available information" to mean information that is lawfully made available from federal, state or local government records. That said, the definition of "personal information" remains very broad and applies to a wide swath of types of data.

Technical corrections: Assembly Bill 1355 provides a number of technical corrections to the CCPA. This amendment clarifies, among other things, that class action lawsuits may not be brought for data breaches when the compromised personal information is either encrypted or redacted (as originally passed, the CCPA had required both encryption and redaction), provides express authority for the Attorney General to establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household, and clarifies the scope of the exemption for data that is covered by the Fair Credit Reporting Act.

Guidance on consumer requests: The amendments also provide guidance on the processes for consumer requests to exercise their CCPA rights. The CCPA originally required all businesses to provide two methods for consumers to submit access and deletions requests, including a toll-free telephone number. Assembly Bill 1564 modifies this requirement for businesses that operate exclusively online and have a direct relationship with consumers: these business are now only required to provide an email address for consumers to make requests to access and delete their data.

Data broker registry: Assembly Bill 1202 requires data brokers to register with the Attorney General, requires the Attorney General to make available a data broker registration on its website, and grants enforcement authority to the Attorney General to seek an injunction and civil penalties against any data broker who fails to register.

The Attorney General's Draft Regulations

The Attorney General's draft regulations, while still subject to public comment and potential amendment before becoming final, are notable because they change and expand businesses' obligations under the CCPA in several key ways. The draft regulations consist of seven articles that run 24 pages in length and relate to nearly every provision of the law. But as discussed below, the most critical draft regulations relate to the purpose of processing, responses to consumer requests, notices and reporting to consumers, and opt-outs.

Purpose Limitation

One of the most significant ways in which the draft regulations go beyond the text of the CCPA is in adding a purpose limitation requirement. Under the draft regulations, if a business intends to use a consumer's personal information for any purpose that was not disclosed to the consumer at the time the information was collected, the business must directly notify the consumer of this new use and must obtain explicit consent from the consumer for this new use. This requirement is relevant to many businesses that have found value in performing analyses on customer information they have already collected, whether for marketing, product development, or other purposes. Machine learning and enhanced data analysis have made these types of analyses common and valuable.

Under the draft regulations, though, if the purpose underlying the follow-on analysis of a consumer's information was not disclosed at the time the information was collected, the business will have to contact the consumer to both notify the consumer of this processing and obtain consent from the consumer. This requirement should lead businesses to

continued on page 11

continued from page 10

analyze their privacy notices closely and take steps to align them with current and anticipated uses of consumers' personal information, because if the initial notice provided at the time of original collection of the data is sufficient, the secondary notification and consent will not be needed. To achieve this goal, the employees who are responsible for drafting privacy notices must coordinate with the operations and marketing personnel who typically derive value from follow-on analyses of consumer information.

Responses to and Verification of Consumer Requests

As discussed above, the CCPA creates a number of rights consumers can exercise with regard to their personal information. The draft regulations establish the procedures businesses must use when they receive requests from consumers to exercise their rights.

Since the CCPA was passed, businesses and commentators have been concerned about the possibility of individuals fraudulently making requests with regard to other people's personal information. So it is notable that the draft regulations provide guidance for businesses on what information to require in a request for purposes of verifying the identities of the consumer making requests. Once the initial request and verifying information have been submitted, businesses are generally to avoid requesting additional information for verification purposes. If, however, the business is unable to verify the requestor's identity, it may request additional information, but the additional information may only be used for verification, and must generally be deleted shortly after the business processes the consumer's request.

If, despite these steps, a business is unable to verify a requestor's identity, the draft regulations require the business to inform the consumer of the fact. Furthermore, if the request is for information disclosure, the business must explain the categories of personal information the business holds, without providing specific data relating to the particular individual who is the subject of the request. And if the request is for information deletion, the business is required to treat the request as a request to opt-out of the sale of that information.

The draft regulations also forbid businesses from disclosing certain types of information in response to CCPA requests: a business cannot disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers. And a business also now has discretion to decline to disclose specific personal information if the disclosure would create a "substantial, articulable, and unreasonable risk" to the security of the personal information, the consumer's account, or the business' own systems and networks. Neither the regulations nor the statute provide guidance as to what factors a business should use to determine the existence of such a risk, however.

The draft regulations also provide some guidance, and introduce some ambiguity, with regard to requests for deletion of personal information. They provide that in response to verified requests for deletion, businesses must de-identify the information, aggregate the information, or permanently and completely erase the information from their existing systems "with the exception of archived or back-up systems." But they also state that, "[i]f a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used." Neither the CCPA nor the draft regulations provide any guidance with regard to determining when an archived or back-up system is "accessed or used," which raises the possibility that any movement of data over to a backup system could create a duty to erase data on that backup system. This is likely an issue that will be addressed during the comment period.

Reporting and Notices to Consumers

As discussed above, when businesses specify a purpose for their data collection in the notice they provide to consumers before or at the time of data collection, the draft regulations prohibit businesses from deviating from that stated purpose. The draft regulations also go farther than the statute by providing that businesses must specify the purpose of collection for each separate category of personal information they collect. They also establish requirements concerning the comprehensibility of consumer privacy notices, requiring businesses to draft them in a way that "provides consumers a meaningful understanding of the information being collected," uses "plain, straightforward language," "avoid[s] technical or legal jargon," and can be read on "smaller screens, if applicable."

The draft regulations also create a new reporting requirement for businesses that annually buy, receive for commercial purposes, sell, or share for commercial purposes the personal information of 4,000,000 or more consumers. These businesses must compile annual statistics on the number of requests they receive from consumers for access to their personal information, deletion of their personal information, or to opt-out of sales of personal information, as well as the business' response to those requests. Businesses must then disclose these statistics as part of their publicly available privacy policies or within a link included in their privacy policies.

Opt-Outs

One of the most significant, and potentially most unclear, new obligations in the draft regulations is a requirement to treat "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism" as requests to opt-out of the sale of consumers' personal information. Neither the CCPA nor the draft regulations provide any guidance on questions, such as what mechanisms a business must use to detect relevant browser plugins or privacy settings,

continued on page 12

continued from page 11

how to verify the identity the user of a browser, or whether to treat changes in consumers' browser settings as an abandonment of the opt-out. This issue is likely to be a topic of public comment, but businesses should begin considering how they will comply with a requirement like this if this draft regulation is implemented as it currently stands.

Additional Issues

In addition to the areas discussed above, the draft regulations touch on many aspects of the CCPA, including the treatment of personal information concerning minors, businesses' record-keeping obligations, information requests concerning households rather than individuals, and the classification of service providers.

As the above discussion should make clear, full CCPA compliance remains a moving target while the draft regulations remain open to comment and change. But businesses can take many steps until then to comply with the law's numerous requirements. We will continue to track developments on these issues as the comment period proceeds and the Attorney General issues final regulations.

This alert was written by April F. Doss, chair of the Firm's Cybersecurity and Privacy Practice, Alexander R. Bilus, vice chair of the practice, Patrick M. Hromisin and Jillian K. Walton, associates in the practice. April can be reached at (410) 332-8798 or at April.Doss@saul.com. Alexander can be reached at (215) 972-7177 or at Alexander.Bilus@saul.com. Patrick can be reached at (215) 972-8396 or at Patrick.Hromisin@saul.com. Jillian can be reached at (412) 209-2537 or at Jillian.Walton@saul.com.

April F. Doss

Patrick M. Hromisin

Alexander R. Bilus

Jillian K. Walton

Does Diversity Drive Innovation in Law?

By Womble Bond Dickinson

An interactive panel hosted by the Association for Corporate Counsel's Baltimore Chapter on October 24 set out to discuss the ways diversity drives innovation both for companies and law firms. Panelists engaged in a moderated discussion led by Nicholas Hawkins, an Associate at Womble Bond Dickinson, and included Taren Butcher, Senior Associate General Counsel at Allegis Group, Inc.; Mary Jones, Senior Counsel of Executive Compensation and Benefits at Hilton Worldwide; Leila Hock, Senior Manager for Legal Department Partnerships & Inclusion at Diversity Lab; and Ellen Gregg, Partner and Vice Chair of Womble Bond Dickinson, LLP.

Hawkins laid the foundation for the conversation by defining both "diversity" and "innovation," and providing statistics on the effect diversity has on producing innovative results. Citing from a Harvard Business Review article, Hawkins stated, "Without diverse leadership, women are 20% less likely than straight white men to win endorsement for their ideas; people of color are 24% less likely; and LGBTs are 21% less likely. This costs their companies crucial market opportunities, because inherently diverse contributors understand the unmet needs in under-leveraged markets."

Hock then opened the discussion with a brief history of The Mansfield Rule, which is a take on the NFL's Rooney Rule and required NFL teams to interview at least one diverse candidate for head coaching positions. Under Mansfield, law firms are required to do the same and "consider 30 percent women and attorneys of color for all leadership roles as well as lateral hiring and promotions to partner," (64 Law Firms Announced As Mansfield Rule 2.0 Certified, Diversity Lab). The second iteration of Mansfield included LGBTQ+ lawyers and also considered how firms were including diverse individuals in firm pitches and requests for proposals.

The conversation then turned to Gregg, who expressed that the event was an opportunity to share the benefits of diversity initiatives such as the Mansfield Rule and how they positively affect the relationship between attorneys and their clients. "Womble has a history of diversity initiatives and practices dating back at least 20 years," said Gregg, a veteran trial lawyer and Vice Chair of Womble Bond Dickinson (US), LLP. "We are pleased to participate in Mansfield as an extension of our core values and diversity initiatives at the firm."

Butcher and Jones then gave examples of how their companies were leading the charge in diversity and the connection between those efforts and innovation. Butcher, for example, sits on the company's Diversity and Inclusion

continued on page 13

continued from page 12

Council, which provides support to the company's diverse employees and serves as a sounding board that provides leadership with input and feedback on the company's diversity and inclusion efforts. Aerotek also sponsors the National Association of Black Engineers conference, along with several other STEM related conference, to demonstrate the importance of sourcing and recruiting diverse STEM talent. Butcher reminded the audience that millennials have surpassed baby boomers as the largest generation (83.1 million versus 75.4 million), and millennials are a more diverse cohort (44 percent are part of a racial or ethnic minority group). Focusing on diversity is just a way to stay competitive, "We don't want to be the next Blockbuster, focused on the norm," stated Butcher.

Yes, engaging in diversity and inclusion initiatives is the right thing to do, but it is also a smart business move. One of the key takeaways from the event was Butcher's comment, "Diversity provides companies the competitive edge to succeed." More companies are realizing that a diverse group of thinkers and problem solvers on any particular issue yields better results. Law firms like Womble are realizing this as well and responding by providing a diverse pool of candidates for client RFPs and staffing client matters with attorneys from a variety of backgrounds and experience levels. "Part of that process is assisting the general counsel of our clients to be strong champions in their boardrooms and successful in their careers," said Gregg. "We have to provide solutions for our clients that help give them that competitive edge they need to succeed."

About Womble Bond Dickinson

Womble Bond Dickinson is a transatlantic law firm with over 1,000 lawyers in 27 UK and US offices. Firm services include Commercial, Corporate, Employment, Pensions, Dispute Resolution, Litigation, Finance, Banking, Restructuring, Insolvency, IP, Technology and Data, Private Wealth, Projects, Construction and Infrastructure, Real Estate and Regulatory Law. https://www.womblebonddickinson.com/us.

Board Leadership