LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 31, Number 6 • September 2016

The New FLSA Overtime Rule

By E. Fredrick Preis, Jr. and Rachael Jeanfreau

The United States Department of Labor (DOL) recently issued its final overtime rule revamping the white collar exemptions under the Fair Labor Standards Act for executive, administrative, professional, and highly compensated employees. This Final Rule, effective Dec. 1, 2016, rolls out major changes for employers, and the DOL estimates that 4.2 million workers will either become eligible for overtime or bring home bigger salaries. As Yogi Berra observed, "The future ain't what it used to be."

This article discusses the Rule's highlights and provides compliance tips for employers to "knock this one out of the park," with Yogi-isms to which we can all relate.

'A Nickel Ain't Worth a Dime Anymore'

The Fair Labor Standards Act (FLSA) requires employers to pay overtime compensation to employees who work more than 40 hours per work week. However, the law exempts bona fide executive, administrative, and professional employees from coverage. To qualify as exempt, employees must meet both a "salary test" and a "duties test."

The Final Rule increases the salary threshold required for executive, administrative and professional employees to qualify as exempt from the law's overtime

continued on page 10

The New FCPA Cooperation Plan

Revitalized Program or Regurgitation of Existing Policy?

By Brett W. Johnson and Jeffrey Scudder

On April 5, 2016, the U.S. Department of Justice (DOJ) issued an Enforcement and Guidance Plan (Plan) concerning the Foreign Corrupt Practices Act (FCPA). While the new Plan could be interpreted as a novel departure from past precedent, careful analysis reveals that it does little to alter or clarify how the DOJ will review cases or reward companies for significant cooperation in addressing anti-corruption global issues.

Background on the FCPA and Previous Agency Interpretations

Administered jointly by the DOJ and the U.S. Securities and Exchange Commission (SEC), the FCPA has two primary components: anti-bribery provisions and accounting requirements. The FCPA makes it unlawful for companies and individuals to make payments of any item of value to foreign officials in exchange for influence or business opportunities; it also requires foreign companies with U.S.-listed securities to follow all applicable accounting provisions. However, payments merely facilitating or expediting the performance of a "routine" governmental action represent a crucial but poorly defined exception. Individuals who violate the FCPA are also subject to a fine up to $2 million and up to five years in prison. However, in practice, the DOJ and SEC have brought relatively few FCPA actions against individuals.

In 2012, the DOJ and SEC released a joint Resource Guide intended to provide information on the FCPA. The Resource Guide highlighted the importance of self-reporting possible FCPA violations and the need to enact an appropriate anti-corruption compliance program. It also identified sources from the World Bank, United Nations and others to help companies maximize their mitigation potential. Finally, it emphasized the importance of conducting risk assessments to determine the level of exposure companies faced simply by having properties, subsidiaries, or even distributors abroad. Thus, the Resource Guide did not alter

continued on page 2

In This Issue

New FCPA Plan

continued from page 1

enforcement practices surrounding foreign transactions, but it did offer valuable insights into how companies might reduce risk in the global marketplace.

In 2015, Deputy Attorney General Sally Quillian Yates released a widely publicized "new" policy announcing increased accountability for individuals involved in any violations of the law, including the FCPA. The memo made clear that combatting corporate misconduct required reaching beyond the corporate veil to hold individuals personally accountable. Consequently, the DOJ unilaterality declared that eligibility for cooperation credit (*i.e.*, reduced sentences and fines) would hinge on the disclosure of *all* relevant facts relating to involved individuals. Specifically, the target company would be required to identify every individual involved in or responsible for the alleged misconduct at issue. This obligation was heightened by inferring that the release of culpable individuals was not possible absent "extraordinary circumstances."

However, due to the low rate of individual accountability when companies civilly or criminally settle, this obligation raised serious concerns about chilling effect and applicability to existing and future investigations. Thus, the DOJ's shifted focus of the FCPA away from "corporations" and trained it on the individuals, which impact is still unresolved.

Now, to further confuse the existing playing field, DOJ has released the *Plan*, which sets forth three steps aimed toward enhancing enforcement, cooperation with investigations, and individual accountability. First, the Department vowed to significantly increase the amount of resources devoted toward detecting and prosecuting violations of the FCPA. This, it hoped, would make clear that FCPA violations that might have gone uncovered in the past are more likely to be uncovered.

Second, the Plan pledged to strengthen coordination between the DOJ and its foreign law enforcement counterparts. This, again, was not a real new development, due to the changes since 9/11 in regard to cross-border cooperation related to criminal activity.

Third, it announced a new pilot program aimed toward promoting greater accountability for culprits of corporate crime by incentivizing companies to have detailed compliance programs, test the programs regularly, and report any suspicious activity through a voluntary disclosure. This included an announcement that "mitigation credit" would be available only if a company disclosed "all" (which is not defined or caveated by a "good faith" standard) facts related to involvement in the criminal activity by the corporation's officers, employees, or agents.

The New (or Old) World Order

The new DOJ Plan represents a recycled version of long-standing policy. First, increased investigation and enforcement has been an objective for years. Mark Mendelsohn, Deputy Chief of the DOJ Fraud Section, previously declared in 2009 that roughly 100 companies were the subject of open FCPA investigations. While this trend might continue to grow based on the Plan, it is hardly novel.

Second, the promise to partner with foreign law enforcement counterparts is a well-established practice. In 2008, the Siemens case highlighted the prevalence of cross-border cooperation among governments concerning anti-corruption investigations. Two other examples include the SEC's acknowledgement of extensive assistance from

continued on page 4

Brett W. Johnson and **Jeffrey A. Scudder** are partners in the Phoenix, AZ office of Snell & Wilmer L.L.P. They can be reached at bwjohnson@swlaw.com and at scudder@swlaw.com, respectively. The authors gratefully acknowledge the assistance of **David Wilhelmsen**, a summer associate.

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

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

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

EU-U.S. Privacy Shield Finalized

By Jonathan Armstrong and André Bywater

The European Commission concluded more than six months of negotiations both within the EU institutions and with the U.S. on July 12 with the announcement that agreement had been reached on the Privacy Shield scheme to transfer data from the EU to the U.S.

What Is the Privacy Shield?

The Privacy Shield scheme was proposed in February 2016 to replace the Safe Harbor scheme, which was struck down by the European Court in the first *Schrems* case (sometimes known as *Schrems 1*) in October 2015. The *Schrems 1* case was brought by an Austrian law student, Maximilian Schrems, against Facebook. Mr. Schrems initially complained to the Irish Data Protection Commissioner about the way in which Facebook was transferring his data using Safe Harbor. The Irish Data Protection Commissioner felt that she did not have the power to investigate, since the European Commission had put the Safe Harbor scheme in place. The court disagreed and also felt that the entire Safe Harbor scheme was unlawful.

The FAQs below look at our initial thoughts on Privacy Shield. We use some technical terms that are explained in our glossary here at http://bit.ly/2b6ybTQ.

Why Did It Take So Long to Agree to a New Deal?

Some might say that the announcement of the creation of Privacy Shield was premature. It became apparent soon after the announcement that the February deal was, at best, a deal to do a deal. An announcement had to be made in February as a deadline set by the Article 29 Working Party (often known as WP29) had expired at the end of January. In February, the European Commission said that it hoped Privacy Shield would be finalized by the beginning of May. Even that seemed ambitious, in part because of the criticism that Privacy Shield received from WP29 in April.

Is There Still Opposition to Privacy Shield?

Yes. While we are yet to see whether WP29 are any happier with the extra concessions the Commission say they have secured from the U.S. Government the Privacy Shield deal will still have its critics. There seems to be confusion as to whether the U.S. administration can deliver its side of the bargain, especially when recent court cases in the U.S. are perceived to have undermined the rights of individuals. Since some of the U.S. side of the deal relies on instructions from the current administration there is also uncertainty as to what a change of administration in the U.S. in January 2017 will bring.

Will Privacy Shield Be Protected By the GDPR?

No. Privacy Shield is not referred to in the General Data Protection Regulation (GDPR) although one of the other methods of data transfer, Binding Corporate Rules (or BCRs) is. The European Commissioner promoting Safe Harbor, Věra Jourová, said in August that Privacy Shield would be reviewed prior to GDPR coming into force, since it was a clear requirement that the U.S. had "equivalent" protection and this protection was likely to have the be improved once the GDPR sets the bar higher.

When Does Privacy Shield Come In?

The European Commission said they intended to have it come in Aug. 1. Companies were able to join the scheme from that date.

Will the U.S. Authorities Play a Greater Role?

Almost certainly. If your company joins Privacy Shield, there is likely to be much more supervision by the U.S. authorities than there was under Safe Harbor. It is not true to say there was no Safe Harbor enforcement (for example the FTC's investigation into TRUSTe), but the European Commission is promising tougher enforcement. On July 12, the Commission said:

> … under the new arrangement, the U.S. Department of Commerce will conduct regular updates and reviews of participating companies, to ensure that companies follow the rules they submitted themselves to. If companies do not comply in practice they face sanctions and removal from the list.

Is Privacy Shield Bullet Proof?

Probably not. Penny Pritzker, the U.S. State Secretary of Commerce, said in announcing the deal on July 12 that she thought it would "withstand scrutiny" and that she had been speaking with the chair of WP29 to try and reduce her concerns. Commissioner Jourová also said she was confident it would survive a court challenge.

In our view, it is unlikely that the concerns about Privacy Shield will disappear so quickly. In addition, there are rumors that Austria, Bulgaria, Croatia and Slovenia abstained from the Article 31 vote and it could be that regulators from some of those countries may also take an interest. Privacy Shield is certainly open to challenge in the same way as Safe Harbor was. In effect, its legal status is similar to Safe Harbor — an adequacy finding from the European Commission. There have been indications of likely court challenges already and the *Schrems 1* case tells us that regulators must have more independence to investigate their concerns. We are likely to see investigations from some of the German Regulators, who have already taken Safe Harbor enforcement action.

In addition, there is likely to be a challenge to the European Court of Justice (the ECJ) over model clauses. This case is already in Ireland, and is a proposed referral to the European

continued on page 4

Jonathan Armstrong and **André Bywater**, a member of this newsletter's Board of Editors, are lawyers with Cordery in London, where their focus is on compliance issues.

Privacy Shield

continued from page 3

Court by the Irish Data Protection Commissioner of Mr Schrems' additional complaints about the way in which Facebook uses model clauses. There have been court hearings in the *Schrems 3* case already, and we understand that counsel for the Irish Data Protection Commissioner flagged the fact that those proceedings might need to be amended to accommodate the inclusion of Privacy Shield.

In effect, it seems that the intention from the Irish Data Protection Commissioner would be that the ECJ looks at the legality of the model clauses and Privacy Shield together. We mention in passing that the *Schrems 2* litigation is not directly relevant to Privacy Shield, but rather concerns potential civil damages claims relating to Facebook's alleged data transfer practices.

While a challenge to Privacy Shield does seem likely, there is no guarantee that would succeed. A differently constituted court on a different day may be more willing to uphold Privacy Shield, especially with the extra effort that both the EU and U.S. have made this time around. Whatever the result, however, there is likely to be uncertainty, since a court hearing may still be two years away.

As well as possible challenges from courts and regulators, it should be remembered that Privacy Shield has a one-year shelf life before being renewed. The European Parliament in particular is likely to be looking carefully at the scheme's first year and may challenge its renewal in 2017.

Should I Even Consider Privacy Shield for My Business?

Probably. Despite its faults, those companies who were in Safe Harbor might find Privacy Shield fairly easy to achieve. It could have some role as part of a mix of compliance measures, although it is unlikely to provide a complete solution on its own. It would be wise to look at the scheme to do a cost-benefit analysis. Privacy Shield is likely to be more costly than Safe Harbor — in part due to higher arbitration costs — but may demonstrate a level of compliance to some of your customers.

What About Brexit?

There was a question at the July 12 press conference to Commissioner Jourová about the effects of Brexit and any likely adequacy decision for the UK. Commissioner Jourová said it was too early to answer this question.

Due to the initial two-year time frame for the Brexit negotiations (which have yet to begin), Privacy Shield will apply to data transfers from the UK at least until any eventual withdrawal from the EU. GDPR will also apply.

What Can I Do?

Clearly, the exact list of actions you will need to take will vary from corporation to corporation. Among the possible actions you could consider would be:

1. Have a plan for data transfer — we have seen from some of the enforcement cases that the lack of a plan is likely to cause difficulties when regulators ask questions;

2. Review Privacy Shield to see if it might work for you, even a system subject to a challenge may be useful for you;

3. Look again at your data flows to determine the following: what information travels from the EU to the U.S. and on what basis? Is it intergroup or is it to third parties? What steps are already in place to make those data flows lawful? You may be able to alter your current data practices to reduce your risk;

4. Consider the other options available to your business including model clauses (recognizing that they are also subject to challenge) and BCRs. The latter do have a new footing in GDPR, and may be more resistant to challenge. BCRs will not be the answer for everyone, however;

5. Review your privacy policy. Some organizations have not reviewed their policy since the fall of Safe Harbor in October 2015. Whichever way you make your data transfers lawful, you should still be reflecting your current practices in your privacy policy.

—❖—

New FCPA Plan

continued from page 2

governments spanning four continents during the Halliburton/KBR settlement, and the DOJ's pledge to a mutual legal assistance provisions in the OECD Convention.

Last, incentivizing self-disclosure, cooperation and compliance programs on the part of companies has been a long-standing policy. The 2012 Guide specifically aimed to encourage voluntary disclosure and compliance programs. The Plan really only reiterates this policy. This is especially the case in light of the DOJ Principles of Federal Prosecution of Business Organizations (USAM Principles), which have long touted the value of cooperation on the part of companies and instructed prosecutors to expend extra energy prosecuting individuals. The DOJ even admits in its own Plan that the United States Sentencing Guidelines already provides for reduced fines for voluntarily disclosers, "full" (again, undefined) cooperation, and acceptance of responsibility. Thus, the substance of the DOJ Plan is scarcely innovative.

The new DOJ Plan in reality may actually discourage the very cooperation it purports to promote by demanding at the outset a higher degree of disclosure than either the USAM Principles or the United States Sentencing Guidelines. The USAM Principles stake eligibility for "cooperation credit" on disclosure of the relevant facts. This stands in stark contrast to the new Plan's call for disclosure of "all facts" related to involvement in the subject activity. Likewise, the Sentencing Guidelines permit a defendant to qualify for a downward departure if voluntary disclosure and acceptance of responsibility occurs. The new *Plan*,

continued on page 9

Contracting with A FinTech Company

By Bryan G. Handlos and Kevin F. Griffith

Your favorite internal client has just messaged you about a new contract that needs a rush review. The counterparty is reportedly one of the hottest new "FinTech" companies in Silicon Valley. You are the master of all things vendor contract-related in your shop, but perhaps this is the first FinTech contract to cross your desk. This article addresses some of the special issues that might be presented by this sort of contract.

What Is FinTech?

"FinTech" is a buzzword. It is commonly understood to refer to a services sector focused on providing innovative online or mobile financial services. Customers are usually consumers. Among the most talked-about consumer-facing FinTech services are Betterment (investment advice), Motif (brokerage), OnDeck Capital (small business lending), SoFi (consumer lending), Venmo (payments) and Personal Capital (financial planning). Nonetheless, commercial customer products also exist. Some leading examples are Zenefits (insurance), C2FO (cash flow management), TransPay (cross-border payments), and Tradeshift (electronic invoicing). Commercial FinTech can be expected to grow. Investments in B2B tech start-ups were up 40% to $11.9B year-over-year through the end of March 2016. FinTech service providers are mostly not banks although it is common for them to partner with banks.

Banks have FinTech offerings too, and they will likely increase their presence in the field in the near term. This article, however, focuses mostly on the issues presented by non-bank FinTech companies. Contracting with a bank would mostly involve different considerations. Frequently, a FinTech service provider is a start-up or recent entrant to the field.

The hallmarks of FinTech are the use of new technology to solve old problems with products that are fast, easy to use and convenient. FinTech products are designed to be very efficient and many are undeniably cool. Automation is maximized and human interaction is typically minimized. Hype is not unheard of, and market capitalization of some companies is stunning. Some FinTech companies see themselves as the wave of the future, destined to put "old-fashioned" banks out of business.

For all the innovation of FinTech service providers, they are probably just another type of vendor for your company, one of hundreds or thousands. Most normal vendor management/vendor contracting issues will be relevant. Are there any special areas of concern for contracting with a FinTech company?

Issues Arising Out of Innovation

Because innovation is key with FinTech, the service provider may be a relatively new company and the service itself is likely new, both in what it is and how it is delivered. The service provider may also be on the smaller side and perhaps still evolving. Newer entrants may be unproven in their ability to scale up or handle a large enterprise. These do not present unique or insurmountable obstacles. As compared with well-established vendors, though, these characteristics may require special attention to up-front diligence, testing, product definition, warranties, and change management.

The Hot Property

Successful FinTech companies can be a hot property. Customers and press may be flocking to them. Success, however recent, may embolden them. This, coupled with a reliance on automation and a general need for speed in all things may result in a service provider that is contractually less accommodating than might be desired. This is especially true of unique products where a competitive offer is not available — yet. These issues cannot really be solved with contract language. They can, however, be managed, particularly with a cooperative client who can help establish a productive working relationship with the vendor at the outset (or who can at least determine whether the product is really so critical to the company that it is necessary to suffer the pain of dealing with a non-accommodating vendor). It bears keeping in mind that not every FinTech company that is a hot property today will survive in that lucky status.

Intellectual Property

Intellectual property issues will of course be important to both counterparties to a FinTech contract. The underlying legal issues may not be that unique, but the context in which they are evaluated may be different as compared to dealing with an established technology vendor. For example, infringement protection is a normal ask from any technology vendor. Does the newness and innovation of the FinTech service provider's offering mean that infringement presents a greater risk? Do the vendor's size and long-term prospects engender confidence in the value of the infringement indemnity the fintech service provider is willing to make?

If the relationship is anticipated to be something more than passive receipt of service in a backroom setting, other ownership and licensing issues may be important. Is the customer likely to be contributing to the evolution of the vendor's product in a meaningful way? What rights, if any, should arise out of those contributions? Is it at least clear that the customer is not fenced out of using its own contributions in the future or in alternative relationships? How will the FinTech product be embedded in the customer's other systems? Has the customer complied with its obligations to other systems' vendors? Are there proper provisions for transition and disentangling systems at the end of the relationship? If the FinTech product has a public facing side, are branding and trademarking issues properly addressed?

continued on page 6

Bryan G. Handlos is a partner and **Kevin F. Griffith** is an associate in Kutak Rock LLP's Omaha, NE office. They may be reached at Bryan.Handlos@KutakRock.com and Kevin.Griffith@KutakRock.com, respectively.

FinTech

continued from page 5

Data

It is not uncommon for FinTech service providers to have an expansive view of the data they want to use or have rights in. The customer whose business is the source of that data may obviously have a different and more proprietary outlook. The FinTech vendor may claim the right to use data running through the FinTech product to support other customers, to develop new products, to market products and for other purposes. Are these rights clear, acceptable and properly limited? Is data ownership clear, along with rights to use data, confidentiality obligations and obligations to return information at the conclusion of the relationship? To the extent that the FinTech service provider is handling transactions or data that involve the customer's customers, these data issues can also take the form of customer and customer list ownership, control and portability issues.

As with any vendor contract, and especially where financial information is at issue, data security is likely to be an important and potentially controversial and risky topic. If the customer is used to dealing with regulated financial institutions as its financial service providers, that customer may want to consider the fact that the FinTech service provider may not be similarly regulated (banks being heavily regulated and supervised with respect to data security). The FinTech service provider is probably not required to have the same data security protections in place. Even if they do, they may not have the same degree of internal control and outside examination of those protections as does a bank.

The Consumer Financial Protection Bureau (CFPB), in March 2016, entered into a $100,000 settlement with digital payment company Dwolla for allegedly misrepresenting how it protected customers' data. The CFPB alleged that Dwolla, which has stated that it has since improved its data security, advertised to customers better data security than it actually had at the time. Data security risks can obviously be mitigated with robust data security provisions in the contract, though likely with considerable resistance from the service provider. Given the significant losses that might result from a data breach, the customer should also consider whether the service provider can realistically be expected to be able to stand behind the commitments it does make in this area.

Regulatory Supervision

Innovative, entrepreneurial fintech service providers may have distinct competitive advantages over their more staid cousins, bank financial services providers. Many of those advantages arise from the lack of significant regulatory supervision. Whatever their faults, bank prudential regulators do offer a valuable public service in helping to assure the safety and soundness and stability of banks. Banks offer a safe and conservative choice as a service provider and are perhaps more likely to be around for the long term. Vendor stability risks may take on more or less significance based on the nature of the product being acquired.

FinTech service providers that offer an application to handle limited data present a different risk profile than those that move money, for example. Contracts can play some role in mitigating these risks (*e.g.*, with financial covenants and reporting, audit rights and termination privileges), but real risk management might mean that vendor management teams need to step up their initial diligence and ongoing supervision beyond what they might require of a regulated financial institution.

Regulatory Compliance

In the competition between FinTech service providers and bank financial service providers, there is ongoing controversy over the degree to which FinTech service providers are or should be permitted to operate free from the regulatory compliance restrictions applicable to banks. While this issue may not be as significant in the business space as it is in the consumer space, customers should at least consider whether the topic is relevant to their situation or the specific product involved.

Although most vendor contracts should probably have a compliance with law requirement, counsel may want to drill down on what that really means for products with material regulatory compliance implications. Is the service provider properly licensed? Is it clear the service provider has responsibility for compliance with substantive requirements applicable to a particular service and what is the extent of that responsibility? Is the service provider attempting to allocate compliance responsibility to the customer? Is the service provider attempting to reserve the right to change prices if the regulatory environment changes?

If the service provider is providing a service that supports a product for which the customer has any consumer regulatory compliance responsibility (*e.g.*, a payment functionality offered to the customer's customers), the customer should consider whether to seek the same sort of protections that banks are required to seek of their similarly situated vendors. This is especially true if there is a directly consumer-facing aspect to the FinTech service. This may involve, among other things, establishing clear expectations about compliance (including prohibitions on unfair, deceptive or abusive activities), rights to obtain and monitor the service provider's policies, procedures and internal controls with respect to compliance, training and internal oversight of compliance, notification of complaints and consequences for non-compliance. *See* CFPB Bulletin 2012-03.

Acquisition, Consolidation Or Worse

As compared with all vendors, it may or may not be fair to suggest that FinTech service providers present any greater degree risk of being acquired, consolidated or going out of business or bankrupt. As compared with bank financial service providers, it is probably fair to suggest that FinTech service providers present a

continued on page 8

Patchwork Paid Sick Leave Laws

How to Ensure Employer Compliance

By Lisa M. Schmid

When it comes to initiating employment legislation, we're living in a time when state and city lawmakers are the change agents. From adopting equal pay legislation to raising the minimum wage or instituting paid parental leave, inaction by the United States Congress has resulted in many states and cities taking matters into their own hands.

One notable example is the recent paid sick leave mandates. To date, five states — California, Connecticut, Massachusetts, Oregon, and Vermont — have adopted paid sick leave laws that affect a significant number, if not all, of the employers in those states. In addition, numerous cities — including New York City, Philadelphia, San Francisco, Seattle, Washington, DC, and most recently, Minneapolis — have adopted paid sick leave ordinances. Adding to the list, many states and cities have recently introduced and/or are contemplating paid sick leave measures. These include but are not limited to — Alaska, Florida, Georgia, Hawaii, Louisiana, Maryland, Michigan, Minnesota, Nevada, New York, North Carolina, Chicago, Los Angeles, and Saint Paul.

The new laws can create administrative and employee relations headaches not only for employers in these jurisdictions, but for those who have locations in multiple jurisdictions or otherwise send their employees to work in these jurisdictions. To help employers understand what to expect and better understand the paid sick leave laws, this article outlines how the majority of the recent paid sick leave provisions operate, addresses common compliance difficulties, and provides insight and counsel on compliance and future planning for all employers.

Lisa Schmid is an attorney with Nilan Johnson Lewis in Minneapolis. She can be reached at lschmid@nilanjohnson.com or 612-305-7549.

Commonalities in the Paid Sick Leave Laws

While these various state and municipal paid sick leave laws differ, most of them are developed with a similar structure that includes the following:

- Broad definitions of "employer" and "employee" for coverage purposes;
- An accrual mechanism;
- Rules regarding permissible use of leave;
- Requirements for handling accrued leave upon an employee's separation from employment or transfer to a new location;
- Record-keeping requirements;
- Notice requirements;
- Carryover allowance mandates; and
- Enforcement provisions, which include investigatory powers, imposition of penalties, and possible civil actions in which damages and attorneys' fees may be recovered.

Definitions

The definition of "employer" varies from jurisdiction to jurisdiction when it comes to which companies are affected, but broadly speaking, the scope is expansive. For example, the state of California and the city of San Francisco include all private employers regardless of business size. Other jurisdictions, like Minneapolis and Philadelphia, do not require the mandated leave to be paid if the employer is small enough, but they still require provision of leave. Some take into account industry sector. Connecticut's law excludes manufacturers whereas Minneapolis' law exempts certain construction workers who receive a state-defined prevailing wage.

As the general trend seems to be toward inclusion of all employers, the definition of covered "employee" seems to be expanding to cover most employees, as well. Minneapolis' recently adopted ordinance is a good example. It includes "any individual employed by an employer, including temporary employees and part-time employees, who perform work within the geographic boundaries of the city for at least 80 hours in a year for that employer."

While the original proposal made some exceptions for very small employers (less than six employees), even those provisions were watered down before the ordinance's adoption. Similarly, Philadelphia's ordinance covers anyone who works within the city for at least 40 hours a year; and the ordinance in Emeryville, CA, requires otherwise eligible employees to work in the city for a mere two hours in one week to qualify for sick leave accrual. As a result of the broadening definition of "employee" under the various sick leave laws, any employer who has workers in a jurisdiction with mandatory paid sick leave, regardless of the employer's actual location, must track those hours worked by its employees in the covered jurisdiction and allow for paid sick leave to be accrued if the hours-worked threshold is met.

Coverage

In contrast to the great variety of coverage definitions, the rules for accrual of sick leave do not actually differ much in most jurisdictions. For the most part, the laws allow employees to accrue one hour of sick leave for every set number of hours they work, and they provide for a yearly cap on accrual that typically ranges from three to seven days. In addition, many of the laws also require employees to wait a certain number of days before they can start using their accrued leave.

Furthermore, the uses of accrued leave outlined in the laws mainly include, but are not limited to, taking time off to: receive preventative care; care for a sick family member or obtain preventative care for a family member; recover from or treat an injury or illness; care for a child whose school or daycare has closed because of inclement weather or for other reasons; or to seek medical attention or other assistance due to domestic abuse or sexual assault. Included in most of

continued on page 8

FinTech

continued from page 6

different risk profile. This difference can be significant depending on the nature of the service and how critical the service is to the customer's business (*e.g.*, is the service a data application or a payment service that moves money?). Mitigating these issues does not involve a much different set of contractual tools than is used in other settings. The key here lies more in the customer identifying the degree of risk presented and answering with an appropriate provision (such as an anti-assignment provision or appropriate termination right) instead of letting a boilerplate provision slide through that will not be helpful to the customer when needed.

Conclusion

Many FinTech service providers offer truly innovative and valuable products, sometimes at highly attractive prices. Like the products of any other vendor, these products will rarely be risk free. Careful upfront consideration of the special risks presented by a FinTech vendor will pay dividends in achieving a useful FinTech contract.

—❖—

Paid Sick Leave

continued from page 7

the current and pending laws is a requirement for employers to wait at least three days until they seek documentation for the leave before alleging potential abuse thereof.

Included in the laws is also the ability to carry over accrued but unused pay, meaning that employees may be able to build a bank of accrued leave. So far, the laws don't require employers to pay the existing accrued balance upon an employee's separation. However, employers may have to retain a terminated employee's accrued balance for a certain amount of time in case the employee returns to employment, at which point the balance must be reinstated. The same is true for employees who transfer to a different location. Their sick leave balances may need to be retained and then reinstituted upon returning to a covered location.

A familiar and favorable detail in the rules is that it does not require employers to adopt additional sick leave if they already provide at least the same amount of paid sick or paid leave. However, employers must still comply with other requirements of the new laws (record keeping and notice provisions, etc.) if those weren't previously accounted for, which means that even more generous employers should take note of the growth of state and local sick leave mandates.

Potential Compliance Challenges for Employers

Needless to say, there is significant room to make compliance errors, and the accompanying legal liability for those who have not taken the time to completely understand the laws and their requirements may be substantial.

It also isn't surprising that employers have recently run into compliance challenges because of the current sick leave laws' patchwork existence. Employers that operate in multiple jurisdictions may need to adopt different policies and accrual systems for each unique jurisdiction. Another solution would be to adopt one system for all employees that fulfills the strictest employer requirements.

Employers that require employees to work in an area with a paid sick leave ordinance in effect may find themselves in a situation where some but not all of their employees are entitled to earn and use paid sick leave. This can cause administrative difficulty and possible employee relations issues. For example, a soft drink vendor located outside of a covered jurisdiction that sends its employees on delivery routes in a covered jurisdiction like Minneapolis or Philadelphia for a few days a week could quickly find itself needing to implement a system to track those employees' covered hours and allow them to accrue and use paid sick leave in accordance with the applicable law. Similar issues could be true for employers who aren't based in a covered jurisdiction but allow employees to routinely work at home when those employees live in a covered jurisdiction.

More portable industries — like food trucks, consulting, health care, and construction — may face some difficulty due to how the paid sick leave laws are structured, as the nature of their businesses require them to send employees where their clients or their work is located.

Employers with employees who work a certain number of hours in an area with a paid sick leave ordinance or industries that require employees to travel to these areas for their clients or work are faced with difficult choices. First, they must determine which employee will receive the shifts that make them eligible. This can result in angered employees and possible disparate treatment claims. To avoid some of these issues, employers have four choices, each of which presents various challenges:

1. Adopt a compliant paid sick leave policy for all employees. This policy may need to comply with state and local laws, depending on where an employer's employees work. For example, if an employer sends employees into San Francisco, whatever policy it adopts must comply with both San Francisco's and California's paid sick leave laws.

2. Develop a paid sick leave system for only covered employees while ensuring that employees are selected for the covered work fairly. This may involve a seniority or rotational system that gives numerous employees access to coverage, or provides other benefits to non-covered employees.

3. Develop a rotational work system that prevents any one employee from reaching the coverage threshold, which may be next to impossible for some employers or in some jurisdictions.

4. End all employees' work in covered jurisdictions. While in some ways this is a simple solution, it also is likely impossible for many, if not most, employers if they want to continue operating their businesses as they do now.

Employers that assume their current paid time off programs are

continued on page 9

Paid Sick Leave

continued from page 8

sufficient under the law may also run into compliance issues. For example, an employer that allows for accrual of paid sick leave but does not allow for accrual quickly enough or does not allow sufficient carryover time may be in violation of the applicable law. The same is true for an employer that meets all other requirements of the law but fails to maintain a terminated employee's sick leave balance for the requisite amount of time or fails to post the required notice. Therefore, it is crucial for all employers who may be affected by a newly enacted paid sick leave law to closely examine their current paid leave policies and programs to ensure full compliance.

Time tracking can also cause compliance concerns. This is especially true for exempt employees who generally don't keep detailed tabs on their work hours. To reduce the administrative burden, employers may need to purchase or develop technical solutions to track hours worked in covered jurisdictions.

Advice for Employers

There doesn't seem to be an end in sight for the wave of paid sick leave laws, and with the nature of the laws being technical, complex, and fraught with compliance challenges, it's advantageous for employers to be proactive and take intentional steps.

The first action to take is to determine if the business and/or which employees are operating in a covered jurisdiction. Employers should consider all risks and develop solutions.

If the business operates in a covered jurisdiction, or if at least of some its employees do, employers should examine the existing policy (if developed) to determine if it's compliant and/or make the needed changes, create and implement a sick leave program if needed, and apply updates to the employee handbook to include the new or revised sick leave program. They should then implement record-keeping mechanisms, ensure proper notice is delivered to employees, and provide needed training to employees who are tasked with administering the program.

In addition, employers should consider hiring competent employment counsel to review their sick leave policies and procedures to ensure compliance, and stay up-to-date with state legislators and city council members regarding the adoption of paid sick leave laws. In the event legislation is in the process of being considered, employers can convene or participate with the local chambers of commerce in meetings to discuss the proposal, attend or testify at hearings on the proposed legislation, and advocate for paid sick leave laws that work for both employees and employers.

—❖—

New FCPA Plan

continued from page 4

then, seems to contradict these existing policies, which infers that the previous policies are no longer applicable. This is unfortunate because the Plan's success depends on voluntary corporate cooperation; yet, it imposes a standard of disclosure of "all," which is well beyond that of the USAM Principles, the Sentencing Guidelines, or practical reality.

Finally, like the DOJ/SEC Guide that preceded it, the new Plan fails to give specific guidance on what type of information a company should disclose to the DOJ. It simply issues a carte blanche call for all facts and instructs prosecutors to make a subjective assessment of whether this was actually done. Meanwhile, even if a company complies with voluntary self-disclosure, full cooperation, and timely and appropriate remediation, the Plan affords no concrete guarantee of subsequent mitigation credit. It simply issues a cryptic pledge that cooperation "may" result in up to a 50% reduction in fines, or a declination of prosecution in certain circumstances. Thus, the new Plan omits any guarantee of a reduced civil or criminal penalty or the upside of spending the extensive resources and disclosing without a full appreciation of "all" the facts that exist.

Compliance, Due Diligence And Cooperation

The Plan does not require a variation in long-standing guidance. A company's counsel must play a pivotal role in any investigation for a variety of purposes. The attorney-client privilege is still essential to determine whether or not a violation has actually occurred.

However, it is a delicate situation to decide whether or not to have the company's legal department handle the investigation or whether to engage outside counsel. The current trend is to engage outside counsel to handle internal investigations of possible criminal acts. If this trend holds, the appropriate company official or committee should provide written instructions and authority to the outside counsel to conduct the investigation.

The practice of conducting internal investigations will also not change, despite the high bar set of having to disclose "all" facts. Often, it makes sense to have an impartial senior management person or an audit committee be the "client" for purposes of business decisions related to the investigation and ensuring full cooperation (if possible once the personal liability of employees is discussed during the *Upjohn* warnings). During the internal investigation, it is good for attorneys to work in teams, especially when interviewing employees. It is important that, before asking questions, counsel explain to the employees whom they represent (*i.e.*, the company) and the purpose of the investigation (*i.e.*, to find those responsible). A full review of all records should be conducted. An assessment of the entire program should occur.

As referenced, the compliance program and senior management commitment (and dedication of resources) to the program are key. To determine what a company should do before an incident occurs, it is useful to consider what the DOJ prosecutors examine when they decide

continued on page 10

New FCPA Plan

continued from page 9

to charge a company. An effective compliance program will help a company successfully avoid an FCPA investigation. While the DOJ does not have formal guidelines for evaluating compliance programs, informal elements include: 1) sound corporate policy; 2) training in regard to the policy and the law; 3) adequate staffing to monitor compliance and possibly an independent internal auditor or oversight committee; 4) proper standard clauses in all international agreements; 5) a reporting system for suspected violations and protection of whistleblowers; 6) delineated disciplinary procedures; and 7) a record-keeping system to ensure compliance with the FCPA.

When a potential FCPA violation occurs, the company should immediately investigate and stop the activity if it seems potentially unlawful. This includes the cessation of further payments to overseas agents and even the suspension of the employees involved. Every alleged or potential FCPA compliance violation should have a documented investigation that is reviewed by an internal and external source to determine if a violation has actually occurred. The DOJ specifically examines post-violation conduct to determine whether to charge a company or the individuals involved with an FCPA violation. Therefore, getting it right is crucial.

Remedial action is also crucial. This essentially requires the company to take the actions it possibly should have taken before the alleged violation, such as implementing an effective corporate compliance program, improving an existing compliance program, and disciplining wrongdoers. Willingness to accept responsibility and take mitigation action weighs heavily in a company's favor under the FCPA.

As recognized by the Plan, voluntary disclosures are a growing trend in FCPA investigations. The possible benefit to voluntary disclosure is that the DOJ might be more likely to enter into a deferred prosecution agreement with the company. However, this cooperation may include an attorney-client privilege waiver and its natural repercussions.

Moreover, some studies suggest there are no tangible benefits associated with voluntary disclosure. The only guarantee surrounding voluntary disclosure under the FCPA, then, is the immense degree of discretion retained by the DOJ. As the DOJ is still grappling with the meaning of the Yates memo, individual liability must be discussed with the company officials. But this always should have been a part of the dialogue with the company's management. As such, a company may have legitimate reasons not to self-report and these concerns should be explored.

Conclusion

The new DOJ Plan holds itself out as a ground-breaking means of prosecuting more individual violators of the FCPA by encouraging corporate compliance. However, in reality, it is little more than a repackaged rehearsal of long-standing DOJ policies and practices. The only difference between the old and new policies is the requirement that companies disclose all facts relevant to all individuals involved in the criminal activity at issue. This largely discourages the very corporate cooperation the Plan seeks to incentivize.

What remains clear is that the DOJ will continue to investigate and prosecute FCPA cases. Companies should take this emphasis seriously and ensure that adequate compliance programs are in place, training on the policies takes place, third-party relationships undergo proper due diligence, and a clear plan is set about how to handle FCPA alleged violations, including possibly taking advantage of the Plan.

—❖—

Overtime Rule

continued from page 1

requirements. As of Dec. 1, to be exempt from overtime, such employees must earn a minimum salary of $913 per week, or $47,476 per year — more than double the old requirement of $455 per week, or $23,660 per year.

The FLSA also has an exemption for "highly compensated employees" (HCEs). The Final Rule increases the required total compensation amount for HCEs from $100,000 per year to $134,004 per year. Of this amount, at least $913 per week must be in the form of a guaranteed minimum salary.

The salary threshold level for the overtime exemption for executive, administrative, and professional employees, as well as the HCE compensation level, will automatically update every three years, beginning on Jan. 1, 2020.

'It's Déjà Vu All Over Again'

The Final Rule did not change the "duties tests" that employees must meet to qualify as exempt from overtime under the FLSA. According to the DOL, the increased standard salary level and automatic updating mechanism will adequately prevent employees from being misclassified as exempt from overtime, including employees who meet the duties test, but who also perform "substantial amounts of overtime-eligible work," such as operating cash registers and stocking shelves. Further, the DOL noted that changes to the duties test would disrupt employer operations.

Therefore, the following duties tests still apply to be exempt from overtime:

1. Exempt executive employees must still have the primary duty of managing the enterprise or a department or subdivision of the enterprise. They must also customarily and regularly direct the work of at least two employees and have the authority to hire or fire, or their recommendations as to the hiring, firing, or other change of status of other employees must be given particular weight.

2. Exempt administrative employees must primarily perform office or non-manual work directly related to the management or general business operations of the employer or

continued on page 11

Overtime Rule

continued from page 10

its customers, and they must exercise discretion and independent judgment with respect to matters of significance.

3. Exempt professional employees must primarily perform work: a) requiring both advanced knowledge that is intellectual in character in a field of science or learning that is customarily acquired by a prolonged course of specialized intellectual instruction (such as doctors, lawyers, certified accountants, and engineers), as well as discretion and independent judgment; or b) requiring invention, imagination, originality or talent in a recognized field of artistic or creative endeavor. Computer systems analysts, computer programmers, software engineers or other similarly skilled workers in the computer field may satisfy the duties test, as well as employees who teach in a school system or educational institution.

4. HCEs must regularly perform at least one of the primary duties of an exempt professional, administrative, or executive employee, and they must perform office or non-manual work. For example, an employee may qualify as an exempt highly compensated executive if he or she customarily and regularly directs the work of two or more other employees but does not meet the other duties requirements for exempt executive employees.

'When You Come to a Fork In the Road, Take It'

The Final Rule presents employers with various choices to maintain the overtime exemptions, including the option to use nondiscretionary bonuses, incentive pay, and "catch-up" payments, to satisfy a portion of the new salary threshold for exempt executive, administrative, and professional employees.

It requires exempt executive, administrative, and professional employees to earn at least 90% of the standard salary level ($913 per week) each pay period. Nondiscretionary bonuses and incentive pay (including commissions) may comprise up to 10% of the new salary standard ($91.30 per week) for such employees, provided that the bonuses and incentives are paid on a quarterly basis or more frequently. Therefore, to meet the standard salary amount ($47,476 per year or $11,869 per quarter), exempt employees may be paid up to $1,186.90 in nondiscretionary bonuses/incentive pay per quarter (13 weeks x .10 x $913.00 = $1,186.90).

Nondiscretionary incentive bonuses are those tied to productivity or profitability and include bonuses based on a specific amount of profits generated, bonuses for meeting set production goals, retention bonuses, and commission payments based on a fixed formula.

In contrast, employers may not count discretionary bonuses toward the standard salary amount. With discretionary bonuses, the employer has the sole discretion to decide whether to award the bonus and set the amount of the bonus, and these decisions are not based on any pre-announced standards.

However, HCEs are treated differently from exempt executive, administrative, and professional employees in this regard, and the Final Rule does not allow employers to count nondiscretionary bonuses and incentive payments toward HCEs' standard salary amount. Because commissions, nondiscretionary bonuses, and other forms of nondiscretionary deferred compensation may already count toward almost two-thirds ($86,528) of the HCE total compensation requirement ($134,004 per year), the DOL decided that such payments may not also count toward their base salary threshold ($47,476 per year).

If an executive, administrative or professional employee does not earn enough in nondiscretionary bonuses or incentive pay in a given quarter to remain exempt, then employers may make quarterly "catch-up" payments of up to 10% of the standard salary level for the preceding 13-week period. Therefore, if an employee does not earn the full $1,186.90 in nondiscretionary bonuses/incentives (including commissions) in a given quarter, an employer can simply pay the difference (up to $1,186.90) no later than the next pay period after the end of the quarter. Catch-up payments only apply to the prior quarter's salary amount, that is, the quarter during which the employee's salary fell below $11,869.

Catch-up payments do not count toward the salary amount for the quarter in which they are paid. If an employer chooses not to make the catch-up payment and the employee falls below the salary threshold, the employee must be paid overtime for any overtime hours worked during the quarter.

The Final Rule explains nondiscretionary bonuses and catch-up payments as follows: Assume Employee A is an exempt professional employee who is paid on a weekly basis, and that the standard salary level test is $913 per week. In January, February and March, Employee A must receive $821.70 per week in salary (90% of $913), and the remaining $91.30 in nondiscretionary bonuses and incentive payments (including commissions) must be paid at least quarterly. If at the end of the quarter the employee has not received the equivalent of $91.30 per week in such bonuses, the employer has one additional pay period to pay the employee a lump sum (no greater than 10% of the salary level) to raise the employee's earnings for the quarter equal to the standard salary level.

However, awarding catch-up payments to meet the standard salary amount could disincentivize employees from working to receive nondiscretionary bonuses.

In contrast to executive, administrative and professional employees, quarterly "catch-up" payments

continued on page 12

E. Fredrick Preis, Jr. and **Rachael Jeanfreau** are attorneys in the Labor & Employment Section of the Breazeale, Sachse & Wilson law firm, which represents management. They can be reached at fred.preis@bswllp.com and rachael.jeanfreau@bswllp.com, respectively.

Overtime Rule

continued from page 11

do not apply to HCEs. They must earn the entire base salary amount of $913 per week during each pay period. Although the FLSA does provide for annual catch-up payments for HCEs, these payments only apply to the amount of their total annual compensation beyond the standard salary threshold ($86,528).

'If You Don't Know Where You Are Going, You Might Wind Up Someplace Else'

To avoid winding up in court or a DOL investigation, employers should consider the following when adapting to the Final Rule:

Determine which exempt positions will remain exempt. Employers should audit currently exempt executive, administrative and professional employees who earn between the current salary threshold ($23,660 per year) and the new salary threshold ($47,476 per year). To remain exempt from overtime, such positions will require a salary bump to $47,476 per year and must meet the duties test for the applicable exemption. Alternatively, employers may reclassify such employees as nonexempt and thus overtime eligible. Employers should also audit employees currently exempt as HCEs to confirm that will satisfy the updated compensation requirements. In light of these developments, it is also a good time for employers to audit all exempt positions to confirm that exempt employees are paid on a salary basis and that they satisfy the relevant duties test.

Inform affected employees and their managers of any changes. Employers should communicate with employees whose status will change to nonexempt from overtime and explain that the new rules require this change. Employers should train these employees how to keep accurate time records and explain that off-the-clock work is not allowed. Employers should also communicate with the supervisors of affected employees regarding these changes and requirements.

Adjust hourly wages. For employees now considered nonexempt from overtime, employers can base their new hourly rates on their previous salaries by reallocating earnings between the regular hourly rate of pay and overtime, so that their total earnings stay about the same. As with all nonexempt employees, the new hourly rates must not fall below the applicable minimum wage, which may vary by state.

Structure employee workloads and work time to suit business needs. Depending on its operations, a business may reallocate work among hourly employees to minimize overtime hours, increase work hours of part-time employees, or hire new employees to work regular work hours, which would decrease the business's overall overtime hours.

Track hours worked, comply with other FLSA requirements, and re-apportion nondiscretionary bonuses. Newly nonexempt employees will need to record accurately their time worked on the employer's time-keeping system. This must include all work time, including time spent working from home, e-mailing, or otherwise working remotely. Employers may prohibit employees from working overtime without prior approval. Although employers may discipline employees for working unauthorized overtime, employees must still record and be paid for all time worked, including unauthorized overtime. Further, when hourly employees receive a nondiscretionary bonus, the bonus must be apportioned back over the workweeks during which it was earned to calculate an adjusted regular rate of pay for overtime purposes. Additional pay is due for workweeks in which employees worked more than 40 hours during the relevant bonus period.

Non-profits may use volunteers. Under certain circumstances, nonprofit volunteers who donate their time to religious, charitable, humanitarian or civic organizations as a public service are not covered by the FLSA and therefore, are not covered by the law's overtime requirements. However, employed individuals may not volunteer time for their own non-profit employer doing the same work for which they are employed.

Public sector employers may use compensatory time off. Public employers, including public higher education institutions, may use "comp time" instead of cash overtime for nonexempt employees who work more than 40 hours per week. Comp time must be provided at the same rate as cash overtime. Therefore, employees must earn at least one-and-one-half hours of comp time for each overtime hour worked. Comp time arrangements must be established before the work is performed and may be in a collective bargaining agreement, memorandum of understanding, or other agreement. Comp time agreements should be in writing and provided to employees in personnel regulations or handbooks. Most public employees may accrue up to 240 hours of comp time. However, employees engaged in public safety, emergency response, or seasonal activity (such as admissions counselors), may earn up to 480 hours of comp time.

Conclusion

To successfully adapt their business operations to the new overtime rule, employers should consult with experienced labor and employment counsel.

—❖—