FOLEY

FOLEY & LARDNER LLP

Top Legal Issues Facing The Automotive Industry in 2017

Prepared by Foley's Automotive Industry Team

FOLEY

FOLEY & LARDNER LLP

TOP LEGAL ISSUES FACING THE AUTOMOTIVE INDUSTRY IN 2017

The automotive industry continued to experience dramatic changes — including legal and regulatory developments — throughout 2016, and the road ahead shows no signs of slowing down. Being at the forefront of these developments will help you anticipate how those changes may impact your business.

Foley's Automotive Industry Team has prepared this report that examines what the litigation, enforcement, and regulatory landscape will look like in 2017. Inside, you will learn about:

- Managing warranty, recall, and commercial contracting risk in 2017
- Identifying the causes of uncertainty regarding antitrust issues, as well as some questions and predictions for the coming year
- Taking steps to minimize potential labor and employment issues sparked by the new administration
- Recognizing the advantages in government contracts for small business concerns
- Knowing the risks of international and domestic compliance issues under the new administration
- Meeting the cybersecurity and telematics challenges presented by connected cars
- Preparing your business for the continued aggressive enforcement by the NHTSA regarding auto safety
- Discerning what bumps in the road may lie ahead for automotive mergers and acquisitions

We hope you find this report both useful and informative. If you have any questions regarding its content or how it may directly affect your business, please contact your attorney or the contributors listed on page 26.

FOLEY & LARDNER LLP

WARRANTY AND COMMERCIAL CONTRACT RISK IN 2017

Managing Warranty and Recall Risk

Some economists are predicting that the United States has hit a peak in new vehicle sales due to weaker-than-expected OEM third quarter earnings. Others are predicting that 2017 will bring another high in new vehicle sales. Along with high vehicle sales, OEMs are also in their second consecutive year of elevated warranty expenses. These elevated OEM warranty and recall costs are likely to continue in 2017. While OEMs continue to pay the largest share of warranty and recall expenses, suppliers can expect to pay a greater per-vehicle share of these expenses.

OEM purchase orders and corresponding general terms and conditions are standard in the automotive industry and contain highly OEM-favorable terms. Exceptions and limitations to supplier warranties are difficult to negotiate. In order to be awarded the business, suppliers typically accept liability for a broad range of costs resulting from non-conforming parts. Accordingly, warranty issues have always been a tension point between suppliers and their OEM customers. However, recent increased publicity associated with recalls and service campaigns likely has contributed to a higher expectation by OEMs on safety, quality, performance, and reliability, which makes warranty and recall costs higher risks for the supply base.

After a warranty issue arises, the supplier also needs to react quickly to identify the root cause, contain problems, and establish clean points. The supplier should assemble a claim management team and identify and retrieve the relevant documents from the OEM and at the company. Suppliers also should ensure that responsibility for warranty claim management is not fragmented across business organizations.

Warranty claims also can be difficult to anticipate and manage. If a claim involves multiple parties, including a tier 1 supplier, an OEM, and a tier 2 supplier, a close working relationship between the OEM and tier 1 supplier is required to identify and document quality issues early and to promptly communicate responsibilities. When a warranty spike occurs, the tier 1 supplier must proactively analyze warranty data from the OEM and request additional documentation supporting the OEM's alleged costs and damages prior to settling any warranty claims. The tier 1 supplier also must understand all contract terms and conditions relating to warranty and recall costs, and must obtain the specific details regarding how liability and related costs were established by the OEM.

If a warranty claim involves one or more tier 2 suppliers, contemporaneous notice of the warranty claim, the notice of any breach, documentation of root cause(s), and documentary support for alleged damages are critical should litigation arise. Witnesses should be interviewed, relevant key documents collected and preserved, a risk analysis performed, and a settlement strategy developed. These steps are critical to ensure that:

- The supplier has the ability to demonstrate that it should only be responsible for paying a certain portion of the total costs
- The tier 1 supplier has the ability to pass through any costs that are the responsibility of the tier 2 supplier
- The tier 1 supplier has the ability to recover additional damages from the tier 2 supplier

Avoiding Common Commercial Contracting Mistakes

With international and domestic supply chain contracts, there is little or no room for error. While some supply chain contracts incorporate negotiated provisions in the form of a letter agreement or a long-term agreement, many supply chain contracts rely on standard purchase order terms and conditions. The result is that supply chain contracts of considerable value and corresponding high risk often receive little attention from in-house or outside counsel.

A failure to ensure that key provisions in a supplier's buy-side contracts mirror those of their customer contracts can lead to hold up situations or unwarranted price demands. After negotiation, issues can arise during the performance of the contract that, if not closely monitored, can lead to increased risk. For example, breakdowns in the supply relationship often can occur when parties fail to respond to purported amendments or modifications, engage in a course of dealing that is inconsistent with contractual terms, or fail to properly document agreements to resolve disputes.

Supply chain contract risk can be managed and mitigated with an aggressive legal risk management strategy. Attention to detail and a periodic review and update of basic commercial contracting documents are a must. This is especially true for a supplier's general terms and conditions of purchase, which may have not been updated in many years. Yearly training courses offered to sales and quality teams on basic principles of contract law, warranties, and the Uniform Commercial Code also can help minimize common mistakes during the negotiation and performance phases of a contract.

The company also should designate a point person to manage the contractual relationship. That person should have and maintain a complete copy of the written contract, including all exhibits, addendums, amendments, and schedules. The person should understand the contract and contract rights, and should respond in a timely manner to performance issues to avoid waiver and supply chain disruptions. All-important written correspondence concerning the contract also should be preserved, organized, and readily available, if needed in the event of any dispute or question regarding a contractual interpretation.

Supply Chain Contracting in Light of Regulatory Changes

Contracting parties should be aware of recent regulatory changes, for example, in the areas of self-driving vehicles, highly automated vehicles, vehicle safety regulations, cybersecurity proposed rules, and guidelines regarding confidentiality provisions. In September 2016, the National Highway Traffic Safety Administration (NHTSA) issued the Federal Automated Vehicles Policy (HAV Policy), which applies to OEMs, and equipment designers and suppliers that outfit any vehicle with automation systems. The HAV Policy requires that these entities:

- Submit detailed safety assessments for each HAV system
- Develop documented processes for testing, validation, and data collection
- Submit identifying information and descriptions of HAV systems to NHTSA

Suppliers will need to be more involved with OEMs in ensuring compliance with the HAV Policy.

In December 2016, NHTSA released proposed rulemaking on Vehicle-to-Vehicle (V2V) communications. The proposed rule mandates V2V communications that enable light vehicles to "talk" to each other to avoid crashes. The rulemaking requires certain security requirements for V2V communications. Additionally, in October 2016, NHTSA also issued non-binding guidelines on cybersecurity for vehicles.

Contracting parties also should ensure that any confidentiality provisions allow for the sharing of information with NHTSA. In May 2016, NHTSA issued a warning to an OEM over a non-disclosure agreement that the OEM required certain of its customers to sign prior to obtaining certain out-of-warranty vehicle repairs. NHTSA issued a warning to the OEM that the agreements implied that customers should not contact NHTSA regarding safety concerns. In response, the OEM modified the language of the agreement. In March 2016, NHTSA also issued a final guidance on best practices for protective orders in civil litigation. The guidance provides that protective orders should contain an explicit provision that allows a party to provide information and documents to NHTSA. In light of these recent regulatory changes, contracting parties will need to consider how liability and risk will be allocated in their commercial agreements, and in the event of litigation, ensure that any protective orders comply with the NHTSA guidelines.

FOLEY & LARDNER LLP

International Contracting

Parties to international contracts will need to consider similar regulatory developments discussed above in applicable foreign countries. In addition, parties should consider venue, choice of law, and alternative-dispute resolution or arbitration clauses prior to entering into contracts with parties abroad. It is imperative that the parties agree on these issues in the underlying contract prior to the emergence of a dispute. A failure to agree on these issues could mean that a party is forced to litigate a commercial issue in a counter-party's home country. This prospect could lead to further risk and uncertainty.

"Neutral" law will vary based on the parties to the contract; however, many parties often agree to apply U.S. law. Other "neutral" law can include German or Hong Kong law. Hong Kong law is based on the common law system and rule of equity. Hong Kong also has its own final appellate body. In the event the parties do not agree on the choice of law, an arbitrator may select the applicable law. If multiple international parties are involved, applicable contracts should have mirrored provisions to ensure all applicable parties set forth their consent to these issues. The parties also should designate the venue for the arbitration, the language of the proceeding, and add a clause regarding recognition or enforcement of an arbitral award.

Please contact John Trentacosta, Mark Aiello, Vanessa Miller, or Andrew Fromm if you would like more detail on these issues, including international arbitration, strategies or training to manage risk in the supply chain, or would like a risk assessment performed on your commercial contracting practices.

FOLEY & LARDNER LLP

2017 ANTITRUST OUTLOOK – A YEAR OF UNCERTAINTY

As 2017 approaches, the antitrust outlook is filled with substantial uncertainty, whether in the United States, the European Union, or elsewhere. This brief article identifies some of the causes of present uncertainty, posits a few questions, and concludes by making some predictions.

New Trump Administration Portends Possible New U.S. Directions

For decades going back at least 50 or more years, U.S. antitrust enforcement has been marked more by continuity than abrupt radical change. During this period, there was a gradual evolution in enforcement trends in the United States. This evolution is best characterized by a movement away from blanket rules of per se legality or illegality (e.g., resale price maintenance and inflexible merger standards), greater emphasis on economic analysis of likely competitive effects, and an attempt to strike a rough balance between too-aggressive enforcement (which inhibits potentially procompetitive conduct benefiting consumer welfare) and too-lenient enforcement (which risks unacceptable competitive/consumer welfare consequences).

A new Republican administration takes office in January 2017. During the political run-up to the election, the now president-elect, Donald Trump, frequently expressed populist themes. He criticized rhetorically "big business" and "special interests." Such stump speeches may suggest that the new administration will take a harder and more restrictive line on certain mergers, as well as unilateral and vertical arrangements. Clearly, the new administration will have the ability to make senior appointments at both the Antitrust Division of the U.S. Department of Justice and the Federal Trade Commission. These officials may well have increased ability to influence the direction of and priorities for enforcement. President-elect Trump frequently "tweets" his distain or opposition to the proposed business conduct of specific companies.

For example, Trump has called out Amazon's supposed "dominance" and the AT&T proposed merger with Time Warner for special consideration.

At the same time, it is important to recognize that U.S. antitrust enforcement is characterized by strong, continuous enforcement priorities. Statistics published by the department annually confirm this trend. The Antitrust Division has for decades aggressively enforced per se anti-cartel conduct. This long-standing effort has generated an increasing number of criminal prosecutions, billions of dollars of fines, and dramatically longer terms of incarceration for individual offenders. The number of grand jury investigations continues to be robust. The number of criminal antitrust cases filed has virtually doubled in the last 10 years. It is highly unlikely that criminal enforcement will be relaxed.

Further, antitrust enforcement often comes from the bottom up rather than from the top down. For example, merger enforcement is most often triggered by mandatory triggered premerger notification requirements, which bring potentially problematic deals to the attention of regulators. Civil enforcement has been often precipitated by customer and/or competitor complaints. Enforcement standards have long been, and continue to be, grounded in a series of widely respected guidelines — e.g., merger guidelines, technology transfer guidelines, health care, and international enforcement guidelines. These enforcement patterns and guidelines will slow any attempt to make radical changes in enforcement.

Finally, the U.S. antitrust enforcement system is subject to strict federal court review that should ensure, at least in the short term, continued respect for judicial precedents on enforcement standards that have evolved over time. On balance, then, while we expect continued populist saber rattling, we predict that slow evolutionary change, rather than radical new directions, will shape enforcement trends in the future.

EU Antitrust Continuity Potentially Threatened by Brexit

In a June 23, 2016, referendum, a majority of voters in the United Kingdom (UK) decided that the UK should exit the European Union (EU). While the outcome has been subject to substantial comment, suffice to say, there has long been growing political, social, cultural, and economic restiveness in the UK about EU policies, rules, and membership obligations leading up to the vote to "leave" the EU, which the UK joined in 1973. The process of Brexit will formally begin early in 2017.

The EU was created through a series of treaties that aimed at increasing economic, social, and political integration. That process of integration enshrined four so-called essential "freedoms" — the free movement of people, goods, services, and capital within a common market. It should be evident that the majority of UK voters favoring Brexit rejected, at least implicitly, many of the founding principles on which the EU was based — harmonization of laws across an ever-increasingly level economic playing field, freedom of business and people to move across national boundaries to work and live, and, most profoundly, the notion that Europeans shared a common destiny.

While competition policy was not the most important priority precipitating Brexit, common competition policy was a fundamental goal in the creation of the European Community and, ultimately, the European Union. That common competition policy is now threatened as the UK exits the EU. A number of examples of such uncertainty may be cited. At the heart of the European merger control is the European Merger Control Regulation (EMCR). As a regulation, it has direct effect throughout the EU (including the UK, of course). The EMCR confers exclusive jurisdiction on the European Commission to investigate and prohibit anticompetitive mergers, acquisitions, and concentrative joint ventures that had a "community dimension." The EMCR provided for "one-stop" shopping that made merger control in Europe more efficient, less costly, and more uniform. Brexit may, depending on the negotiated terms of the exit, reduce the utility or availability of the one-stop shop.

The current EMCR provides a mechanism for the European Commission to take jurisdiction over deals not having a community dimension under certain stated circumstances. UK exit may diminish the value of this provision and will likely result in parallel proceedings in the UK and the EU, with the potential for conflicting outcomes (as reflected in the different enforcement approaches in the EU and the United States on the unilateral conduct of major technology companies like Microsoft, Google, and Apple).

This same kind of problem arises with respect to international cartel enforcement. Like the United States, the EU has had a very aggressive and effective enforcement campaign. Total fines over the five years have exceeded € 8.6 billion, with over € 3 billion to date in 2016. Brexit makes continued cartel enforcement more complex. There is a significant risk of dual prosecution of the same alleged illegal activity, the possibility of multiple fines and penalties being imposed, and the risk of inconsistent outcomes in these parallel proceedings. In addition, there are serious questions of procedure and policy. It is unclear how investigations will be conducted, documents and information collected, confidentiality protected, etc. Open questions relate to the potential conflicting criminal and civil regimes, lenience, and lenience plus, as well as the potential erosion of the protections of the attorney-client privilege.

Finally, Brexit may well make more complex rules, regulations, and enforcement of vertical arrangements. The EU has pursued a rigorous (some say inflexible) approach on exclusive dealing in its efforts to create and foster a single common economic market. A major issue on the EU radar screen at present relates to restrictions in online markets. EU rules on such restrictions have increasingly become stricter as the size and economic importance of online marketplaces have grown. However, many manufacturers (particularly

of luxury goods) restrict retailers from selling online. There is a major case pending before the EU Court of Justice that focuses squarely on this issue. Here again, Brexit may undercut the ability to achieve a common enforcement approach on this significant sector of economic activity.

In summary, 2017 appears to be shaping up as a year in which competition policy and enforcement will face increased uncertainty and complexity.

FOLEY

FOLEY & LARDNER LLP

AUTOMOTIVE INDUSTRY: HOT LABOR AND EMPLOYMENT ISSUES FOR 2017

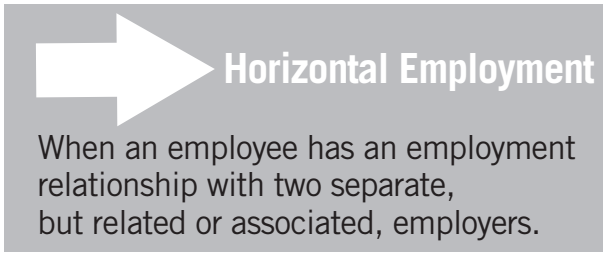
In 2016, employers experienced more aggressive oversight from the U.S. Department of Labor (DOL), the National Labor Relations Board (NLRB), and the Equal Employment Opportunity Commission (EEOC), and struggled to keep up with the onslaught of new regulatory requirements advanced by the Obama administration during its final months. However, the electoral victory of Republican candidate Donald Trump is likely to result in a philosophical shift away from federal oversight and toward a more business-friendly approach to employment regulations.

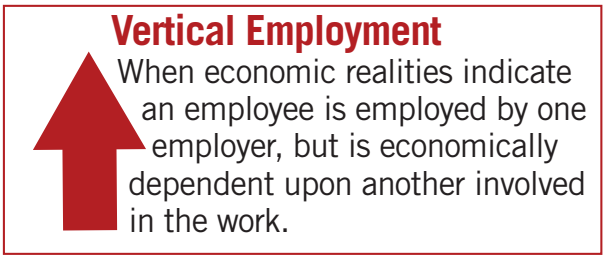
Indeed, President-elect Trump has been vocal about rolling back President Obama's executive orders and his plan to allow states to determine whether or not to implement employment-related regulations. But this does not mean that automotive industry employers should be quick to celebrate. To the contrary, many states and municipalities have already passed employee-friendly legislation and regulations designed to supplement the benefits and protections available under federal law, and these measures may increase if the Trump administration pursues a "hands-off" approach to business regulation. With that in mind, below is a list of questions that employers should be mindful of heading into 2017, along with steps that can be taken to minimize potential risk.

1. Have you evaluated joint employment risks?

If you currently hire contract workers, utilize staffing agencies to supplement your workforce, or share employees with a parent, subsidiary, affiliate, or other employer, 2016 brought with it an increase in joint employment concerns as the DOL joined the NLRB's efforts to move away from the traditional view that joint employment turned on the degree of actual control an entity exercised over a worker and toward a joint employment standard that is "as broad as possible."

Specifically, a 2016 administrative interpretation from the DOL describes "horizontal" and "vertical" employment and outlines a number of factors to be considered for each. According to the DOL, horizontal employment exists where the employee has an employment relationship with two separate, but related or associated, employers (e.g., a manufacturer and a supplier) that are sufficiently connected to be deemed joint employers of an employee. In contrast, vertical joint employment exists where the economic realities show that the employee is employed by one employer, the "intermediary employer," but is economically dependent on another employer involved in the work. Examples of intermediary employers include staffing agencies and subcontractors.





An expansive definition of joint employment could create unprecedented potential liability for employers. When joint employment exists, each employer is jointly and severally liable for unpaid wages and overtime. All the hours an employee works each week for each joint employer is aggregated and considered as one employment. Similarly, each employer may be held liable for discrimination, retaliation, failure to provide benefits required by law, or other violations of labor and employment laws.

Although Trump appointees could eventually revisit and revise these broad agency interpretations of joint employment, auto industry employers and others with supply-chain, franchising, subcontracting, or staffing relationships should review any agreements and arrangements with such entities to assess whether a joint employment relationship exists under the current expanded definition. If you determine that a joint employment relationship exists, consider whether this is an effective business arrangement, assess the DOL and NLRB factors to avoid conditions that might lead to a joint employment determination, and conduct due diligence on the other entity. At the very least, you should confirm that the other entity is correctly compensating its employees and is compliant with key labor and employment laws. You should also consider indemnification provisions to provide an additional line of defense in the event that one or both companies are sued by the shared worker.

2. Do you have any pay equity concerns?

Both the EEOC and the Office of Federal Contract Compliance Programs (OFCCP) have identified systemic gender pay discrimination as a key area of focus for 2017 and, although both agencies have struggled in recent years to unearth substantial evidence of actual discrimination in pay, numerous workplace studies document a chronic wage gap between male and female workers. Additionally, Ivanka Trump, who by all accounts is one of the president-elect's closest advisers, has promised that her father will "fight for equal pay for equal work." Accordingly, employers need to take some action now to ensure that they are prepared for any potential enforcement efforts in this area.

Employers who are not in compliance with the Equal Pay Act face considerable risk. Under the Equal Pay Act, as well as Title VII, an employee may file a pay discrimination claim alleging he or she is not receiving equal pay for equal work. If, for example, a female employee demonstrates that she was paid differently than a male employee for performing work requiring the same skills, experience, and responsibilities, the employee may be entitled to significant damages, including back pay. If the wage disparity is proven to be intentional sex-based pay discrimination, the employee may also be entitled to liquidated damages equal to the amount of back pay awarded. The potential for class actions alleging pay disparity exponentially expands the potential legal liability.

This topic has received plenty of press as numerous Fortune 500 companies have pledged to monitor overall compensation, as well as hiring and promotional practices, in order to remedy pay disparities. Additionally, recently passed regulations will require many employers to incorporate pay data in their annual EEO-1 reports. Specifically, as of March 31, 2018, federal contractors and other employers that employ more than 100 workers will be required to include information regarding W-2 wages and hours worked with the demographic information already provided in EEO-1 reports. Because EEO-1 reports are available to government agencies, as well as the public, these requirements are designed to provide greater visibility regarding potential gender or race/ethnicity-based disparities in pay. The EEOC and OFCCP are also hoping that the new data-gathering requirement will encourage employers to voluntarily analyze and address any pay disparities.

Given the burdens associated with the new EEO-1 reports, these reporting requirements are prime targets for rollback or amendment in advance of the 2018 reporting date. However, the EEOC is still likely to investigate and pursue wage discrimination cases even under a Republican administration. In light of the EEOC's ongoing focus on pay disparities and the additional data that may eventually be available to government agencies and the public, employers should review their current pay systems and conduct a comprehensive pay equity analysis. Any such review should be completed with the assistance of counsel (in order to maintain the attorney-client privilege) and should, at minimum, analyze whether there are gender, race, or ethnicity-based disparities in compensation.

3. Are you in compliance with Form I-9 and employment eligibility requirements?

On November 14, 2016, the U.S. Citizenship and Immigration Services (USCIS) issued a revised version of Form I-9, Employment Eligibility Verification. Employers are required to complete this form for every employee hired who performs work in the United States. Employers may continue using the current Form I-9 (with a revision date of 03/08/2013) through January 21, 2017. However, beginning on January 22, 2017, employers must use the new revised form.

It is critically important that employment eligibility information obtained during the onboarding process is accurate and comprehensive. Effective August 1, 2016, the U.S. Department of Justice (DOJ) implemented substantial increases in I-9 fines for failing to complete the form or completing it incorrectly. Under the new fine schedule, employers face penalties such as the following:

- I-9 paperwork violations: $216 – $2,156 per Form I-9
- Knowingly employing unauthorized alien (first offense): $539 – $4,313 per violation
- Knowingly employing unauthorized alien (second offense): $4,313 – $10,781 per violation
- Knowingly employing unauthorized alien (third or more offenses): $6,469 – $21,563 per violation
- E-verify employers — failure to inform the Department of Homeland Security of continuing employment following final non-confirmation: $751 – $1,502 per violation

The DOJ also increased penalties for document abuse and unlawful employment practices. Employers are prohibited from discriminating against individuals based on their citizenship or immigration status or based on their national origin in the Form I-9 process. For example, employers must accept any document an employee presents from the I-9 List of Acceptable Documents, as long as the document reasonably appears to be genuine and relates to the employee. Employers are prohibited from asking for a specific document or for more or different documents after an employee has already presented qualifying I-9 documents.

Penalties for document abuse and unfair immigration-related employment practices include the following:

- Document abuse: $178 – $1,782 per violation
- Unfair immigration-related employment practices (first offense): $445 – $3,563 per violation
- Unfair immigration-related employment practices (second offense): $3,563 – $8,908 per violation
- Unfair immigration-related employment practices (third or more offenses): $5,345 – $17,816 per violation

Although predictions are difficult to make, we anticipate the Trump administration will have a substantial impact on immigration laws. We anticipate an increase in I-9 auditing and enforcement by the USCIS. Consequently, employers should take action now to ensure compliance with I-9 documentation and processes. In addition, during his campaign, President-elect Trump promised to mandate that E-Verify be used by employers to confirm the immigration status of every American worker. He is also expected to make changes to the H1-B visa program for foreign nationals. Employers should watch for these potential changes in the future.

4. Other Anticipated Hot Topics in 2017

Other anticipated hot topics for 2017 include paid sick leave; evolving lesbian, gay, bisexual, transgender, and queer (LGBTQ) rights; and reasonable accommodations for religious practices, disabilities, and pregnancy.

Paid sick leave will continue to be a hot topic. Effective January 1, 2017, certain federal contractors entering into new covered contracts will be required to provide one hour of paid sick leave for every 30 hours worked, up to 56 hours (seven days) in a year. Although momentum for a federal paid sick leave was growing prior to the election of Donald Trump — and Trump, himself, has suggested that he may require employers to provide six weeks of paid maternity leave for new mothers — it remains to be seen whether the president-elect will support paid leave efforts or take action to roll back sick leave requirements, including the new requirements for federal contractors. Either way, employers will still have to deal with a variety of paid leave laws as we continue to see an expansion of such laws during 2016, with paid sick leave benefits now mandated or in the process of implementation in several states (including California, Connecticut, Massachusetts, Oregon, and Vermont) and localities (including Chicago, Minneapolis, New York City, Portland, San Diego, Seattle, and most recently, Washington, D.C.). In 2017, these laws will continue to cause compliance difficulties for multistate employers given the varying requirements and lack of consistency from location to location.

The rights of LGBTQ employees in the workplace will continue to be a hot topic in 2017, as the law in this area continues to evolve. In the past two years alone, the U.S. Supreme Court has upheld same-sex marriage as a constitutional right, the EEOC has litigated and obtained settlements in cases over the issue of whether discrimination based on gender identity or sexual orientation violates Title VII, and the Obama administration enacted regulations to protect workers who are employed by, or seeking jobs with, companies doing business with the federal government from sexual orientation or gender identity discrimination. Additionally, in its Strategic Enforcement Plan for 2017 – 2021, the EEOC identified protecting LGBTQ people from discrimination based on sexual orientation as an emerging and developing priority, and the United States Court of Appeals for the Seventh Circuit could be the first federal appellate court to determine that Title VII protects against job discrimination based on sexual orientation. Consequently, employers are encouraged to stay ahead of this trend by developing and enforcing policies prohibiting discrimination and harassment based on sexual orientation and gender identity and expression, in addition to other protected characteristics.

Finally, automotive employers should be mindful of the duty to accommodate applicants and employees based on pregnancy, disability, and religious practices. In its Strategic Enforcement Plan for 2017 – 2021, the EEOC identified accommodating pregnancy-related limitations under the Americans with Disabilities Act Amendments Act and the Pregnancy Discrimination Act as an emerging and developing priority, and it published guidance on discrimination based on national origin and related religious views. Likewise, courts continue to focus on the employer's duty to accommodate and the particular burdens of requested accommodations. Therefore, if you suspect that an employee is experiencing difficulty performing his or her job due to pregnancy, a potential disability, or a religious belief, the best course is to proactively discuss the situation with the employee and, when appropriate, provide the needed accommodation and/or otherwise begin the interactive process. Training managers and human resources personnel are also key to ensuring that the interactive process occurs and reasonable accommodations are identified and thoroughly evaluated in appropriate circumstances.

FOLEY & LARDNER LLP

GOVERNMENT CONTRACTS: ADVANTAGES FOR SMALL BUSINESS CONCERNS

Spending over $425 billion in fiscal year 2016, the federal government is the largest purchaser of goods and services in the United States. The U.S. government has a goal to award 23 percent of U.S. government contracts to small business concerns. To assist federal agencies in meeting these statutory small goals, the Small Business Administration (SBA) administers a number of programs to promote contract awards to certain types of small businesses.

Collectively, these programs provide a number of advantages to small business concerns in federal government contracting and present a significant business opportunity for small businesses in the automotive sector. Further, large business concerns with government contracts, including those in the automotive industry, are encouraged to subcontract with small business concerns and, in some circumstances, are required to set small business subcontracting goals and periodically report to the federal government on their achievement of such goals.

What is a Small Business Concern?

Under the Small Business Act, a "small business concern" (SBC) is defined as a business that is "independently owned and operated and which is not dominant in its field of operation." Under SBA regulations and the Federal Acquisition Regulation (FAR), to qualify as an SBC, a business cannot exceed the small business size standard for the relevant procurement action. The SBA size standards are based on either the company's number of employees or their annual receipts. Importantly, when calculating the number of employees and annual receipts for size purposes, the SBA regulations and the FAR require the contractor to include all domestic and foreign "affiliates" in the calculations.

These affiliation rules prohibit a large business concern from creating a wholly owned subsidiary and designating it a small business concern. The SBA regulations and the FAR provide additional detailed guidance regarding what factors could cause entities to be affiliates of one another for size purposes, such as common management, facilities, and employees. Companies must closely review these regulations to ensure accurate calculations and small business certifications.

A number of SBA programs aim to create federal contracting opportunities for specific types of SBCs, including the:

- 8(a) Business Development Program
- Veteran-Owned Small Business Program
- Service-Disabled Veteran-Owned Small Business Program
- Women-Owned Small Business Program
- Historically Underutilized Business Zone (HUBZone) Program

Note that in order for a business to qualify for one of these small business categories, the concern must first qualify as an SBC, as described above.

Advantages for Small Business Concerns

The FAR requires contracting officers to set aside acquisitions over $150,000 for SBCs when there is a reasonable expectation that at least two offers from SBCs will be obtained and an award will be made at fair market prices. Set-aside contracts and the set-aside portion of partial set-aside contacts include FAR clause 52.219-14, Limitation on Subcontracting. FAR clause 52.219-14 requires that an SBC itself perform a certain percentage of the set-aside contract, or set-aside portion of a partial set-aside contract. Depending on the type of contract, the SBC must perform at least 15 – 50 percent of the cost of the contract.

In May 2016, the SBA issued a number of changes to the Limitation on Subcontracting requirements, including a new methodology for calculating the "50 (or 15) percent rule," focusing on the total payments by

the government to the prime contractor, as opposed to the cost of contract performance. Further, the revised regulations allow small business prime contractors to count work performed by "similarly situated entities" as worked performed by the SBC, by excluding work performed by the similarly situated entity from the meaning of subcontracted work for purposes of determining compliance with the applicable limitation on subcontracting.

The SBA administers a number of different government-sponsored mentor organizations and resource programs. One of the major SBA mentoring programs is the Mentor-Protégé Program, which aims to develop strong protégé firms through business development assistance provided by a mentor and to help protégé firms successfully compete for federal government contracts. The SBA issued a series of changes to the program in July 2016, transforming it from a series of programs for each type of small business to a single, all-inclusive mentor-protégé program principally modeled on the SBA's 8(a) Mentor-Protégé Program. Under the new program, large business concern "mentors" will help enhance the capabilities of small business concern "protégés" by providing assistance on several fronts, including management and technical, financial and contracting assistance, trade education, business development assistance, and general and/or administrative assistance.

Small Business Subcontracting Requirements or Large Businesses

FAR clause 52.219-8, Utilization of Small Business Concerns, sets forth the U.S. government's policy that SBCs "shall have the maximum practicable opportunity to participate in performing contracts let by any Federal agency, including contracts and subcontracts for subsystems, assemblies, components, and related services for major systems." Prime contractors and subcontractors are required to carry out this policy in awarding subcontracts "to the fullest extent consistent with efficient contract performance." Additionally, prime contractors must establish procedures to ensure timely payment to SBCs in accordance with the terms of their subcontracts with SBCs. Prime contractors and subcontractors are also required to cooperate in any studies or surveys that may be conducted by the SBA or the awarding agency as are deemed necessary to determine the extent of the contractor's compliance with the clause.

The subcontracting assistance program requires large business concerns awarded prime contracts and non-commercial item subcontracts in excess of $650,000 (or $1,500,000 for a contract for construction of a public facility) that offer further subcontracting opportunities to submit a small business subcontracting plan (Plan) to the appropriate contracting agency. A Plan requires the large business to establish small business subcontracting goals, includes the steps the large business plans to take to achieve those goals, and specifies periodic reporting requirements regarding the percentage of small business subcontracts awarded as compared to the company's established goals.

Compliance

Compliance with small business subcontracting requirements is essential for both large and small businesses. In addition to affecting a contractor's eligibility and ability to compete for federal acquisitions, misrepresentations of size status can lead to criminal fraud charges or civil False Claims Act liability for entities that provide such false information. Further, willful misrepresentations of size status are deemed to result in a total loss to the government, and a contractor can be assessed damages in the amount of the total contract award, even if the contract was otherwise fully performed to contract specifications. A small business prime contractor can be subject to significant penalties for failing to comply with FAR clause 52.219-14, Limitation on Subcontracting, in small business set-aside prime contracts, including suspension or debarment from future federal government contracting. As a result, it is critical that both large businesses and SBCs are aware of the SBA's laws and regulations governing the small business programs referenced herein, and ensure that small business certifications are accurate when submitted, in particular taking into account the SBA's affiliation rules.

FOLEY

FOLEY & LARDNER LLP

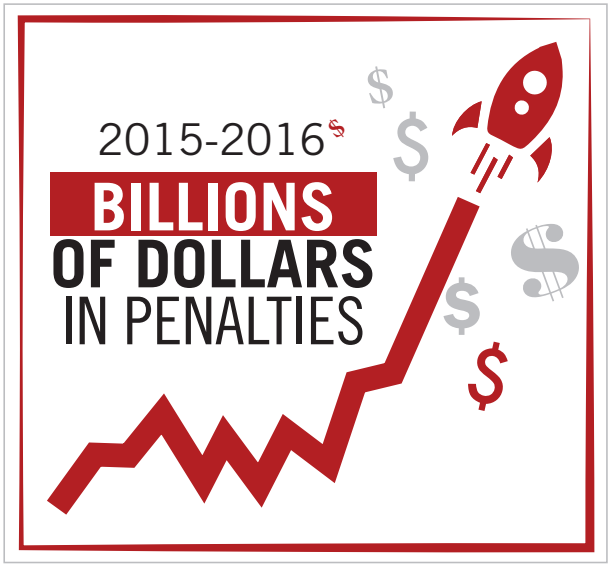
KNOW THE RISKS: UNDERSTANDING INTERNATIONAL AND DOMESTIC COMPLIANCE ISSUES

The aggressive enforcement of U.S. laws governing exports and international conduct is amply illustrated by the continuing imposition of large penalties on multinational companies for violations of U.S. economic sanctions and export control laws, with the last two years imposing billions of dollars of penalties as enforcement activity skyrocketed. While the enforcement priorities of the incoming administration are not yet set, it is highly likely that enforcement of the international regulatory regime will continue to receive high-level attention and that the large penalties will continue under the new administration.

The U.S. government has undertaken a strategy of aggressively enforcing U.S. laws governing extraterritorial conduct. These include the Foreign Corrupt Practices Act (FCPA), economic sanctions largely administered by the Office of Foreign Assets Control (OFAC), and export controls on U.S. goods. These laws underscore the premium that all multinational companies need to place on aggressively identifying and managing regulatory risk, particularly for their international operations.

The automotive sector is a high-profile industry, resulting in amplified risks and a higher level of special enforcement and regulatory attention. In addition to the well-publicized antitrust enforcement actions that have targeted the industry, high-profile FCPA investigations involving prominent original equipment manufacturers (OEM), and special OFAC sanctions that target the automotive sector and any such operations in Iran, underscore the risks that automotive suppliers incur when selling or operating overseas. Similar developments are evident in the domestic domain as well, where the growing frequency and intensity of antitrust, False Claims Act, and government contract investigations present new challenges for manufacturers, suppliers, and service providers of all kinds.

Many automotive companies — reading the headlines and not the actual changes in the law — have mistakenly concluded that the recent easing of sanctions with regard to Cuba and Iran mean that these countries are "open for business." This is especially true with regard to their non-U.S. operations, which often have only a hazy understanding of how aggressive and creative the U.S. government is with regard to applying these laws abroad. The reality is, the primary sanctions remain in place for both countries (especially Iran), meaning that the risk of dealing with these countries remains high. Further, with President-elect Trump indicating that he intends to take a tough stance with regard to Iran (and potentially with regard to Cuba), care in all operations with sanctioned countries, governments, and individuals is especially important in the current uncertain political environment.



From misconceptions of the scope of the easing sanctions to maintaining compliance in the areas of international regulations, managing these international issues on a piecemeal basis is a recipe for failure and

frustration. Instead, automotive suppliers can better manage their risk and mitigate costs by adopting a risk-based approach to compliance tailored to their unique method of operations, risk profile, countries of operation, and products sold. The starting point is ensuring that the organization is aware of the parameters of what the law requires, puts in place compliance measures to deal with identified risk, and that it continually monitors what are expected to be significant changes in the parameters of the international regulatory regime imposed by the U.S. government.

Greater Risk Awareness Leads to Greater Exports and International Compliance

U.S. laws governing exports and international conduct pose unique risks for the automotive sector. From the FCPA to ever-changing sanctions and export controls, companies involved in the automotive supply chain face an increasingly complex universe of requirements governing how and where they conduct business overseas. These regimes also shape business decisions at home, with the so-called "deemed export" rule compelling exclusively domestic companies to seek export licenses before disclosing controlled articles, data, software, and technology to their non-U.S. employees. Combined with disclosure requirements for listed companies and government contractors, the regulatory environment grows more complicated with each passing day.

Enforcement trends amplify these risks. In recent years, U.S. government agencies have targeted automotive and automotive supply chain companies under a number of different regulatory regimes. Notable examples include FCPA enforcement actions against AB Volvo, Daimler AG, Fiat, Iveco, Ingersoll-Rand, and Renault. The revelation of ongoing FCPA investigations within the industry, such as the disclosure by Delphi Corporation in its SEC filings that it is investigating potential FCPA violations in China, underscores that the regulatory risks posed by foreign operations are real and not going away any time soon. Sanctions enforcement is also on the rise, with Toyota Motor Credit Corporation and Volvo Construction Equipment North America both targeted by the U.S. Treasury Department's Office of Foreign Assets Control. Automotive companies like GM-Daewoo have even faced government enforcement actions in relatively obscure areas like anti-boycott violations — a little-known legal regime that has both export and tax implications.

The importance of compliance also is underscored by the 2015 announcement by the U.S. Department of Justice that it will require companies to identify individuals who participated in the conduct at issue in each of their investigations. The goal is to bring an element of personal liability and responsibility into enforcement actions. Given that all the laws that have major enforcement activity (FCPA, OFAC sanctions, export controls, antitrust, and anti-money laundering) all have resulted in criminal convictions of individuals, this increased focus on identifying persons who participated in violations is a sobering reminder of the stakes that arise from poor compliance with these laws.

Many companies in the automotive sector have attributes that contribute to elevated risk. Chief among them are large global supply chains, downstream manufacturing by worldwide affiliates, and frequent international trade in U.S. goods, services, and technologies. Multinational business practices also raise concerns, with sales, operations, and joint ventures reaching into countries known for high levels of corruption, industrial espionage, and illegal export diversion. With U.S. companies increasingly liable for the actions of their overseas agents and affiliates, a risk-based, integrated approach to international compliance offers the best means of identifying, managing, and mitigating these risks.

Develop a Comprehensive Approach to International Compliance

Faced with these challenges, automotive companies should carefully consider how U.S. laws impact behavior both within and outside the United States. This means identifying and addressing the risks that are likely to arise based on the nature of their business, the places where they conduct business, and the customers they serve. It also means evaluating the degree to which foreign parties — whether subsidiaries, joint ventures, or even contractors — engage in activities that expose their U.S. counterparts to civil and criminal liability. By

taking a comprehensive approach, companies can best manage their risk and mitigate costs by conducting periodic risk assessments, crafting tailored internal controls, conducting frequent training, and coordinating common standards across their entire organizations.

The same principles apply in the domestic compliance context. Suppliers need to understand their areas of risk and rigorously monitor and enforce their compliance policies, procedures, and codes of conduct. Conducting periodic internal reviews, reviewing and updating written policies and procedures, and updating and enhancing training programs are all components of a robust compliance program. Encouraging your employees to report any improper, unethical, or illegal conduct is critical to uncovering any potential fraud within your organization. Clearly delineating responsibility for compliance with various policies and internal controls ensures accountability.

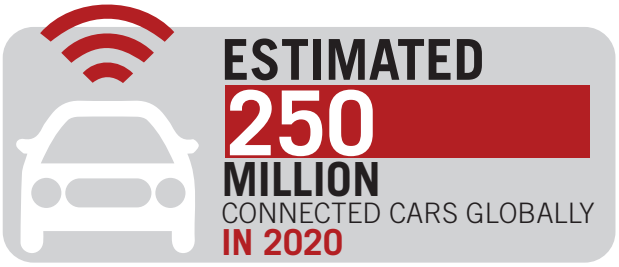
FOLEY & LARDNER LLP

MITIGATING RISKS RELATING TO CYBERSECURITY AND TELEMATICS

Today's marketplace has given connected cars the green light. As an OEM or supplier accelerating to create products to meet industry demand, what challenges can you anticipate in 2017?

Data Protection

The manufacturing industry is now one of the most hacked industries. While onboard infotainment and telematics systems provide rich features desired by consumers, they also bring new legal and compliance risks in the form of potential privacy and security pitfalls and landmines. Autonomous and highly automated vehicles add to the complexity and risks.



It has been said that the modern-day car is a computer on wheels. That is not quite right. The modern-day car is a network of several computers on wheels. Cars today can have 50 or more electrical control units (ECUs) — each of which is analogous to a separate computer — networked together. These ECUs control everything from the car's stereo system to its breaking and even ignition systems. There will be an estimated 250 million connected cars on roads around the world by 2020. These cars will have 200 or more sensors collecting information about us, our cars, and our driving habits.

With significant advances in smartphone car connectivity and onboard infotainment systems, our cars are collecting more and more information about our daily lives and personal interactions. As a result, privacy and security of connected cars has evolved and quickly risen over the last year to a top priority of carmakers and suppliers. Recognizing the importance of these issues, the automotive industry established an Information Sharing and Analysis Center (ISAC) to facilitate the exchange of cybersecurity threats, countermeasures, and other information relating to the security of connected cars.

The ISAC serves as a central hub for gathering intelligence that allows automakers and suppliers to analyze, share, and track cyber threats and spot potential weaknesses in telematics and other vehicle electronics. In July 2016, the Auto-ISAC published its *Automotive Cybersecurity Best Practices.* In October 2016, the National Highway Transportation Safety Administration (NHTSA) published its own *Cybersecurity Best Practices for Modern Vehicles*. The following are what we believe to be some of the most useful takeaways from these best practices.

1. Practice "security by design." This is a concept recently espoused by federal regulators, namely, the National Highway Traffic Safety Administration and the Federal Trade Commission, as well as industry self-regulatory organizations. With security by design, a company addresses data security controls "day 1," while products, components, and devices are still on the drawing board. Data security practices evolve over time, and the days of building it first and then layering security on top are now over. Risk assessments addressing potential threats and attack targets should be dealt with during the design process. Security design reviews and product testing should be conducted throughout the development process. Secure computing, software development, and networking practices should address the security of connections into, from, and inside the vehicle.

2. Practice "privacy by design." While security deals with the safeguards and measures implemented to protect the data from unauthorized access or use, privacy

focuses on the right and desire of individuals to keep information about themselves confidential. During the design process, companies should understand and identify what personal information will be collected by a component or device; what notice should be provided to or consent obtained from consumers before collecting that personal information; how the personal information should be used; are those intended uses legal; with whom will the personal information be shared; and is that sharing appropriate and legal. With this information identified, the company can reconcile privacy requirements with security safeguards during the design and development process.

3. Establish an appropriate data security governance model. Executives and senior management can no longer blindly delegate data security to the security engineering team. Regulators, courts, and juries are demanding that senior management become involved in and accountable for data security. While the precise governance model will depend on the nature and size of the organization, the company should actively consider what level of executive oversight is appropriate, and then document those conclusions in a data security governance policy. This will serve the dual purposes of enhancing the data security of vehicles and component parts, while also bolstering the company's defenses in the event of a security incident or investigation.

4. Address the entire supply chain. Whether it is the finished vehicle or a component part, most companies relevant to the data security ecosystem will rely on suppliers that play a role in data security. Hardware, software, development tools, assembly, integration, and testing may all be provided by one or more suppliers. Companies impacted by this scenario should conduct appropriate due diligence and risk assessments with respect to its suppliers, both at the commencement, as well as periodically throughout, the relationship. Contractual provisions should also be utilized to address data security requirements for the relevant suppliers.

5. Incident response and recovery. Companies should develop and implement a security incident response plan. These plans identify what the organization should do if it or its products are the victim of a data security incident — a potential or actual breach of security impacting the confidentiality, integrity, or availability of data. The data may be sensitive confidential information of the company or its business partners, or may be the personal information of consumers. The plan should address not only the company's own networks, but also its products, if any of them impact the confidentiality or security of data. An incident response team should be in place to coordinate an enterprise-wide response to a cybersecurity incident. The plan should be periodically tested through incident simulations in order to promote response team preparedness.

6. Education and awareness. An educated workforce is crucial to improving the cybersecurity posture of motor vehicles. Cybersecurity educational activities should not be limited to the current workforce or technical individuals, but should also enrich the future workforce and non-technical individuals. NHTSA encouraged educational competitions that include cybersecurity elements such as the SAE/ Battelle Cyber Auto Challenge, the National Institute of Standards and Technology's National Initiative for Cybersecurity Education program called out in the 2014 Cyber Enhancement Act (PL113-274, Title IV), and the Enhanced Safety of Vehicles Student Design Competition.

Conclusion

The reality is that absolute security can never be guaranteed in complex systems such as telematics and infotainment systems in cars. The Auto-ISAC and NHTSA best practices properly assume there will be exploitable vulnerabilities and provide guidance for dealing with that reality and responding quickly. Automakers and suppliers involved in developing infotainment, telematics, and communications systems can never relax and need to stay vigilant in order to keep our cars safe from cyber attacks.

FOLEY

FOLEY & LARDNER LLP

NHTSA AND MOTOR VEHICLE SAFETY

Following the multitude of consent orders, record penalties, and soaring recall numbers the industry has seen in recent years, 2016 was another active year for NHTSA. The agency appears poised to continue the aggressive posture it has taken, even as the current secretary of the U.S. Department of Transportation, Anthony Foxx, and current NHTSA administrator, Mark Rosekind, depart at the end of the Obama administration.

Continued Aggressive Enforcement

Under the Fix America's Surface Transportation Act (FAST Act), signed into law in December 2015, NHTSA's funding will increase significantly over the next few years. NHTSA appears poised to use some of that funding to expand staffing levels within the agency's Office of Defects Investigation. NHTSA's enforcement offices are in the midst of a substantial reorganization, with the likely effect of institutionalizing the aggressive posture that the agency has adopted under the Obama administration. Indeed, Dr. Rosekind has publicly stated that the agency has put in place a number of career officials to continue the current posture after he departs the agency.

Cybersecurity

As the technologies in vehicles race forward, there are growing concerns with how the public could be affected. In April 2016, NHTSA published a request for comments on its enforcement guidance concerning safety-related defects and emerging vehicle technologies. 81 Fed. Reg. 18,935 (Apr. 1, 2016). Through the non-binding guidance document, NHTSA staked out its position with respect to regulating emerging technologies. In evaluating whether a defect poses an unreasonable risk to safety, NHTSA has stated that it will apply its traditional analytical framework — "the likelihood of an occurrence, the severity of the harm, the known engineering or root cause, and other relevant factors" — to these new technologies. (81 Fed. Reg. at 18,938). Importantly, NHTSA has taken the position that it has statutory authority to regulate software installed on motor vehicles.

NHTSA outlined the factors it will consider in evaluating cybersecurity threats as potential safety-related defects:

- The amount of time elapsed since the vulnerability was discovered (e.g., less than one day, three months, or more than six months)
- The level of expertise needed to exploit the vulnerability (e.g., whether a layman can exploit the vulnerability or whether it takes an expert to do so)
- The accessibility of knowledge of the underlying system (e.g., whether how the system works is public knowledge or whether it is sensitive and restricted)
- The necessary window of opportunity to exploit the vulnerability (e.g., an unlimited window or a very narrow window)
- The level of equipment needed to exploit the vulnerability (e.g., standard or highly specialized)

NHTSA POSITION ON CYBERSECURITY Vulnerabilities:

No actual incident in the field is necessary to exercise its authority.

In reviewing the likelihood of an occurrence, NHTSA's position with respect to cybersecurity vulnerabilities is similar to its position with respect to traditional safety-related defects, i.e., it need not wait for an actual incident in the field to exercise its authority.

In October 2016, NHTSA published its long-awaited Cybersecurity Best Practices for Modern Vehicles (Report No. DOT HS 812 333 (Oct. 2016)). The underlying principle stressed by NHTSA is that the industry should "make vehicle cybersecurity an

organizational priority." NHTSA believes that developing layered protections for the vehicle reduces the probability of successful attacks and mitigates the ramifications of unauthorized access to a vehicle's electronic architecture. This layered approach should focus on protecting safety-critical vehicle functions (e.g., brakes, steering, acceleration) and personal information; timely detection and responses to potential vulnerabilities; methods to quickly recover from the vulnerability; and a process to institutionalize lessons learned from across the industry. NHTSA recommends that the industry also look to standards and best practices already developed in the broader information-technology-security industry, such as the ISO 2700 series of standards and the Center for Internet Security's (CIS) Critical Security Control for Effective Cyber Defense, which are used in the financial, energy, communications, and IT sectors.

In developing these recommended processes, the industry should focus on designing systems free of unreasonable safety risks and protecting privacy. NHTSA recommends that the industry explicitly consider the entire life cycle of the vehicle — conception, design, manufacture, sale, use, maintenance, resale, and decommission. The life-cycle approach poses a difficult challenge as the state of technology rapidly changes, while the average vehicle life has begun to climb in recent years.

NHTSA's guidance suggests policies that manufacturers should consider putting into place in order to demonstrate that they are in line with the best practices in this area. Specific practices that NHTSA will likely expect the industry to engage include evidence that the manufacturer has allocated resources to specifically address these concerns, communication channels that ensure vulnerabilities are reported to the appropriate parts of the organization, "an independent voice for vehicle cybersecurity" within the design process, and "top-down emphasis" on cybersecurity within the organization. Guideposts for demonstrating these practices include:

- Participating in the Automotive Information Sharing and Analysis Center (Auto-ISAC), which became fully operational in January 2016
- Developing policies around reporting and disclosure of vulnerabilities to external cybersecurity researchers
- Instituting a documented process for responding to incidents, vulnerabilities, and exploits and running exercises to test the effectiveness of these processes
- Developing a documentation process that will allow self-auditing, which may include risk assessments, penetration test results, and organizational decisions
- For original equipment, developing processes to ensure vulnerabilities and incidents are shared with appropriate entities throughout the supply chain
- As vehicle technologies continue to progress, we expect that NHTSA's guidance will evolve to address future concerns

Automated Vehicles

- Automated technologies hold great promise to improve vehicle safety by preventing driving errors. As these technologies advance, two themes have emerged: the need to introduce automated technologies safely and public acceptance of these potentially life-saving technologies. Federal and state regulators play a large role in these changes.

In September 2016, the U.S. Department of Transportation and NHTSA jointly released a much anticipated federal policy statement concerning automated vehicles, titled *Federal Automated Vehicles Policy, Accelerating the Next Revolution in Roadway Safety* (Sept. 2016). This policy statement outlines their approach to accelerating the introduction of highly automated vehicle functions across the U.S. fleet. The policy recognizes that the introduction of automated technologies is inevitable; that early guidance can help achieve significant safety improvements; and that many of the unknown variables of today will become well known as these technologies progress.

The policy outlines a general framework for developing automated technologies, which should be applied to both test and production vehicles. In particular, entities involved in this segment of the industry need to develop a description of the Operational Design Domain (ODD), Object and Event Detection and Response (OEDR), and the fall-back minimum risk condition. The policy

encourages entities to develop a clearly defined ODD and map the system to the level of automation defined by SAE Standard J3016. To aid NHTSA in monitoring highly automated vehicles, the agency requests that manufacturers and other involved entities provide reports regarding how they are following the guidance. This "Safety Assessment Letter" should cover:

- Data recording and sharing
- Privacy
- System safety
- Vehicle cybersecurity
- Human-machine interface
- Crashworthiness
- Consumer education and training
- Registration and certification
- Post-crash behavior
- Federal, state, and local laws
- Ethical considerations
- Operational design domain
- Object and event detection and response
- Fall back (minimal risk condition)
- Validation methods

Along with the Federal Automated Vehicles Policy, NHTSA published enforcement guidance related to automated technologies. 81 Fed. Reg. 65,705 (Sep. 23, 2016). Responding to comments to NHTSA's April 1, 2016, proposed enforcement guidance, NHTSA focused the final guidance solely on automated technologies. The agency noted that its long-standing practice has been to use its rulemaking authority to set safety standards when new technology has been developed and proven. NHTSA considers systems and equipment related to vehicle automated technologies to be motor vehicle equipment within NHTSA's authority, whether they are offered as original equipment, after-market equipment, or as improvements to original equipment. It also considers software (including programs, instructions, codes, and data used to operate computers and related devices) and after-market software updates to be motor vehicle equipment.

With respect to whether a motor vehicle or equipment poses an unreasonable risk to safety, NHTSA stated that it will consider the vehicle component or system involved in a potential issue, the probability of an occurrence, frequency of the hazard, severity of the hazard to the vehicle and occupant, known engineering or root cause, and other relevant factors. The agency also reiterated its long-standing position that manufacturers need to design around foreseeable misuse of equipment. Likely due to the highly publicized accident involving a semi-autonomous driving system, the agency stated that such a system that does not anticipate distracted or inattentive drivers may be an unreasonable risk to safety. This example stresses the need for manufacturers to make evaluating human factors part of their product development.

Importantly, NHTSA believes that failure to design software that will last for the life of its associated equipment or failure to provide secure updates could constitute a safety-related defect. Of course, it remains to be seen how the agency's enforcement approaches will play out in the real world.

NHTSA's V2V Communications NPRM

On December 13, 2016, NHTSA floated its long anticipated Notice of Proposed Rulemaking (NPRM), which proposes to require vehicle-to-vehicle (V2V) communication in all light-duty vehicles. (The NPRM will be officially published in the Federal Register on January 12, 2017.) The proposed rule follows the Agency's Advanced Notice of Proposed Rulemaking (ANPRM), published in 2014, that sought comments from the industry and public exploring technical, legal, security, and privacy issues related to implementing V2V communications.

In the NPRM, the Agency proposes to issue a new federal motor vehicle safety standard (FMVSS) No. 150 that would require new light vehicles to be capable of sending and receiving "Basic Safety Messages" to and from other vehicles. The messages would be broadcast using short-range radio communication (DSRC) devices and would transmit information about a vehicle's speed, heading, brake status, and other information to surrounding vehicles. As the technologies surrounding automated vehicle functions progress, NHTSA holds

to its view that V2V communications will play a complementary role to these technologies, allowing vehicles to "see" around corners and through other vehicles and transmit this information to surrounding vehicles. In addition to vehicle positional and behavioral data, V2V and so-called vehicle-to-infrastructure (V2I) communications also could potentially transmit environmental data, such as road conditions, to surrounding vehicles.

NHTSA understands that successfully deploying V2V technologies requires a great deal of coordination among a wide range of participants within the industry and government, and that the Agency is uniquely positioned to facilitate the coordination through its rulemaking authority. In particular, NHTSA proposes to mandate the use of DSRC communications within the 5.850 to 9.925 MHz band (governed by the FCC under 47 CFR Parts 0, 1, 2, and 95 for onboard equipment and Part 90 for roadside units) using IEEE 802.11p for the physical and data link layers. With respect to the message format, NHTSA is proposing standards consistent with SAE 2735 and SAE 2945 related to data elements such as speed, heading, trajectory, etc. NHTSA also proposes standards for authenticating communications, hardware security, and procedures for detecting and reporting device functionality to ensure it has not been altered or tampered with. The agency is not proposing specific V2V safety applications at this time, opting to allow standardization and hoping that as the technology is the technology becomes more widely adopted, it will tackle safety applications.

FOLEY

FOLEY & LARDNER LLP

THE 2017 AUTOMOTIVE MERGERS AND ACQUISITIONS OUTLOOK

Another year, and we are further away from the all-time high in valuations and deal activity we witnessed in 2015; but despite signs that the extended expansion cycle for the industry may be plateauing, automotive appears poised to remain a leading sector for M&A activity through 2017. Prognostics for macroeconomic factors are mixed. There is a consensus that the long-anticipated series of interest rate hikes by the Federal Reserve (which began in December) is forthcoming, which would dampen the availability of debt financing for potential buyers.

However, so long as the generally positive outlook for global economic growth is realized (driven in part by a strengthening U.S. economy), we hope that any downturn in deal activity for 2017 will be modest at worst. Opportunities in hot sectors such as connected and autonomous driving, electric vehicles and lightweight material technologies, as well as throughout the general component supplier market, should continue to entice buyers to remain active in the market so as not to be left sitting on the fences. However, the days of a continuing upward trajectory of deal multiples across the entire industry appear to be over, at least for the near term.

Valuation Multiples are Coming Back to Earth

Deal multiples have fallen from the highs of 2015. According to PricewaterhouseCoopers (PwC), during the first six months of 2016, the average EBITDA (earnings before interest, taxes, depreciation, and amortization) multiples for deals in the automotive industry (including public company valuations) was 6.7x, down from 9.9x in the first half of 2015, including a 42 percent drop in the vehicle manufacturing sector. Certain sectors have seen values rise, such as a component suppliers 34 percent increase year over year, but the overall trend has been downward from the rocketing valuations we experienced in 2015. A key open question for 2017 is whether the deal multiples will stabilize or continue their downward trajectories. While lower multiples typically reflect lower demand overall, in a positive growth environment they can lead to pendulum swings upward as buyers (especially private equity firms and other financials) spot value opportunities, as assets are more attractively priced.

Interest Rates are Expected to Continue to Rise in 2017

The surge in deal activity in the past few years has been fueled in no small part by sustained historically low interest rates that have provided buyers with access to cheap money. With solid economic reports and unemployment rates continuing to drop, we entered 2016 with Federal Reserve officials predicting four rate increases during the year. The first and only increase of the year occurred in December. If the Federal Reserve decides to move forward with its long-anticipated series of interest rate hikes through 2017, we can expect overall deal activity to slow as buyers who typically rely on debt to facilitate dealmaking, such as private equity investors, are faced with a raised interest scenario that they have not been in for some time.

The Trump Card: What Impact Will Trade Policy Changes Have on the M&A Market?

The largest wildcard that may impact M&A activity in 2017 is the uncertainty relating to trade policy

changes from the new Trump administration. Certainly, potential changes to NAFTA will be a centerpiece of that uncertainty, given the heavy flow of component parts and assembled vehicles among U.S., Mexico, and Canada; but other factors, such as possible changes in America's relationships with China and the continuation of the Brexit could all have major impacts on deal activity as companies and investors in the industry hold their collective breath for some clarity as to how drastic these changes may be and in what direction global trade policy is headed. Uncertainty is generally bad for dealmaking as it makes business due diligence more troublesome, and sometimes that uncertainty can drag down or delay decision-making. The impacts of any trade policy changes will continue to be watched closely as we enter 2017.

Smart Car, Electric Battery, and Self-Driving Technologies Continue to Drive Activity

Perhaps the highest profile development in the automotive M&A market in the past few years has been the increase of deal activity driven by emerging technologies in smart cars, electric vehicles, connected and autonomous driving, and ride sharing. From the major automakers down through supply chain, manufacturers, suppliers, and technology and start-up companies traditionally outside of the automotive space have raced to invest in, acquire, and develop these technologies.

General Motors made headlines with its recent $1 billion acquisition of autonomous vehicle developer Cruise Automation. In October 2016, the second largest technology deal in history, Qualcomm's acquisition of chip maker NXP Semiconductors for a staggering $39 billion, was driven in large part by developments in the smart car market. In a recent article Bloomberg quoted Dietmar Ostermann, director of the automotive practice at PwC, warning that "If you don't buy now, and boost your capabilities for autonomous driving and for connected cars, there's no second chance — because the others will." Everyone is, and we can expect this trend to continue in 2017.

Light Weighting is In

Deal activity in the vehicle light weighting area has been strong. According to a 2016 special report on vehicle light weighting published by McKinsey & Company, the prices that OEMs are willing to pay for lighter weight are likely to continue to rise. The McKinsey & Company report cited several contributors to this trend, most notably the government-mandated fuel economy standard requirements, which in the United States currently targets a 54.5 mpg fleet average by 2025. The federal government's recent pronouncements in the closing days of the Obama administration that it is not inclined to relax this timeline as part of its mid-term review likely will cause automakers to stay on course for a 2025 date, pending more definitive guidance on the issue from the Trump administration.

One of the most important deals of the year in this space is Teijin Limited's recent agreement to acquire Continental Structural Plastics Holdings Corporation (CSP), a major composite supplier based in Michigan, for $825 million. CSP is the world's largest sheet molding compound manufacturing for automakers and has developed advanced technologies in the lightweight composite arena such as glass fiber reinforced plastic. Teijin Limited's acquisition of CSP should be seen as part of a growing trend as carbon fiber's use in vehicles continues to grow. According to a survey by WardsAuto, light weighting and improving the efficiency of engines are the two technologies at the top of the list for manufacturers to improve their fleets' efficiency over the next decade. The demand for advances in this space should drive deal activity and valuations in 2017 and beyond.

FOLEY

FOLEY & LARDNER LLP

CONTRIBUTORS

Subscribe to Foley's ***Dashboard Insights*** blog (autoindustrylawblog.com) for the latest in industry legal news.

For more information on emerging legal and business developments for the automotive industry, please contact:

WARRANTY AND COMMERCIAL CONTRACT RISK IN 2017: MANAGING WARRANTY AND RECALL RISK

Mark Aiello
Partner
Detroit, MI
313.234.7126
maiello@foley.com

Vanessa Miller
Partner
Detroit, MI
(313) 234-7130
vmiller@foley.com

John Trentacosta
Partner
Detroit, MI
313.234.7124
jtrentacosta@foley.com

Andrew Fromm
Associate
Detroit, MI
313.234.7162
afromm@foley.com

2017 ANTITRUST OUTLOOK – A YEAR OF UNCERTAINTY

Howard Fogt
Partner
Washington, D.C.
202.672.5378
hfogt@foley.com

AUTOMOTIVE INDUSTRY HOT LABOR AND EMPLOYMENT ISSUES FOR 2017

Carmen Couden
Partner
Milwaukee, WI
414.297.5568
ccouden@foley.com

GOVERNMENT CONTRACTS: ADVANTAGES FOR SMALL BUSINESS CONCERNS

Erin Toomey
Partner
Detroit, MI
313.234.7138
etoomey@foley.com

Kimberly O'Brien
Special Counsel
Detroit, MI
313.234.7151
kobrien@foley.com

KNOW THE RISKS: UNDERSTANDING INTERNATIONAL AND DOMESTIC COMPLIANCE ISSUES

Gregory Husisian
Partner
Washington, D.C.
202.945.6149
ghusisian@foley.com

Christopher Swift
Senior Counsel
Washington, D.C.
202.295.4103
cswift@foley.com

MITIGATING RISKS RELATING TO CYBERSECURITY AND TELEMATICS

Chanley Howell
Partner
Jacksonville, FL
904.359.8745
chowell@foley.com

NHTSA AND MOTOR VEHICLE SAFETY

Christopher Grigorian
Partner
Washington, D.C.
202.672.5542
cgrigorian@foley.com

R. Nicholas Englund
Special Counsel
Washington, D.C.
202.295.4792
nenglund@foley.com

THE 2017 AUTOMOTIVE MERGERS AND ACQUISITIONS OUTLOOK

Steven Hilfinger
Partner
Detroit, MI
313.234.7123
shilfinger@foley.com

Joshua Munro
Associate
Detroit, MI
313.234.7189
jmunro@foley.com

About Foley

Foley & Lardner LLP provides award-winning business and legal insight to clients across the country and around the world. Our exceptional client service, value, and innovative technology are continually recognized by our clients and the legal industry. For 13 consecutive years, Foley has been recognized on the BTI Client Service A-Team, a client service survey of *Fortune 1000* corporate counsel (2016 BTI Client Service A-Team survey, The BTI Consulting Group, Wellesley, MA). In addition, Foley received 27 national Tier 1 rankings in the 2016 edition of *U.S. News – Best Lawyers®* "Best Law Firms," and was named to the *InformationWeek* 500 list for seven of the past eight years for technological innovation that enhances business value. At Foley, we strive to create legal strategies that help you meet your needs today — and anticipate your challenges tomorrow.

Foley.com

FOLEY

FOLEY & LARDNER LLP

BOSTON · BRUSSELS · CHICAGO · DETROIT · JACKSONVILLE · LOS ANGELES · MADISON · MIAMI · MILWAUKEE · NEW YORK · ORLANDO · SACRAMENTO
SAN DIEGO · SAN FRANCISCO · SHANGHAI · SILICON VALLEY · TALLAHASSEE · TAMPA · TOKYO · WASHINGTON, D.C.