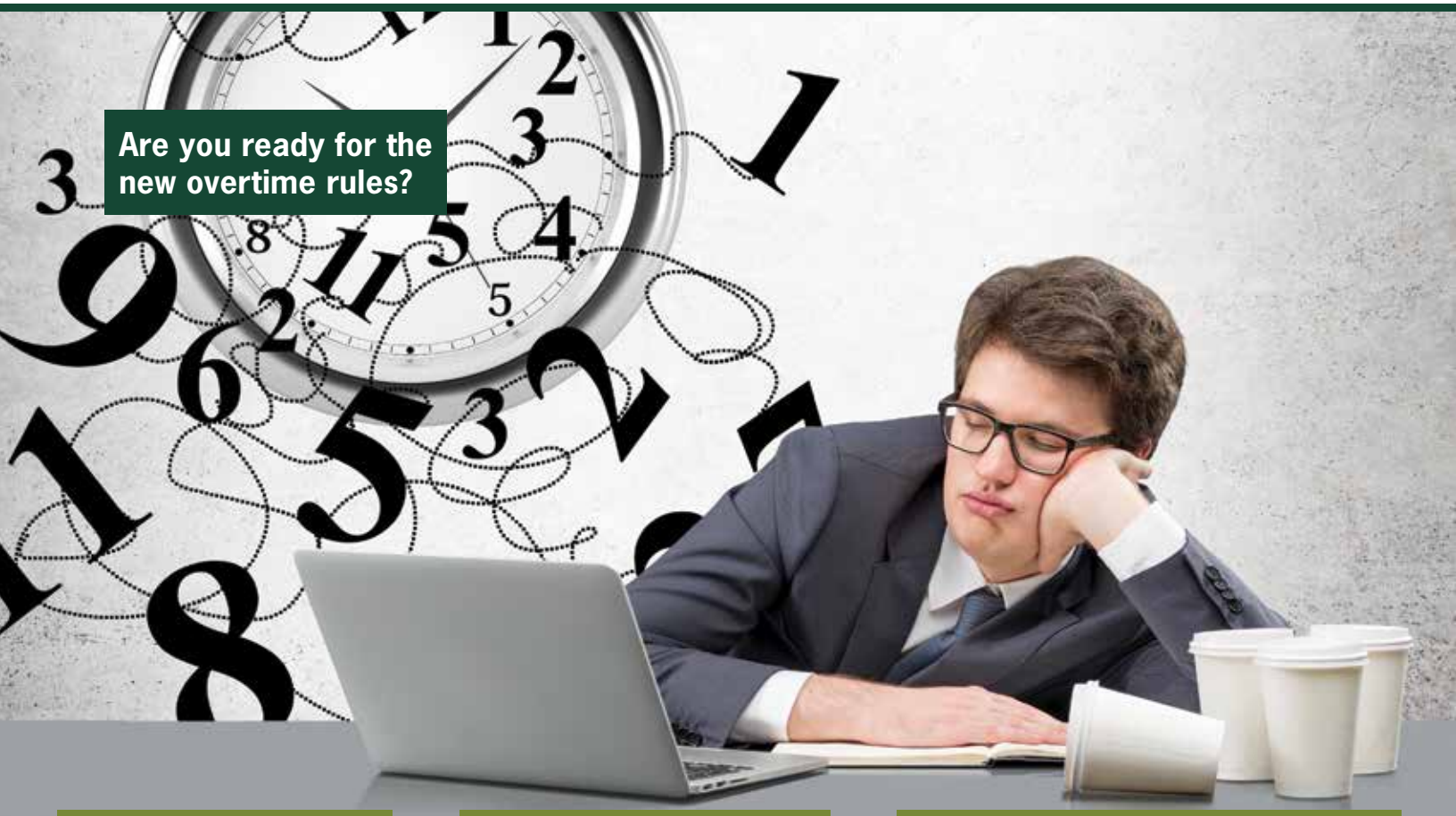
MANUFACTURER

Fall 2016



Are you ready for the new overtime rules?

Spotlight on fraud in the manufacturing industry

Understanding tax issues related to shareholder loans

Cyberrisks mount
Preventive measures for manufacturers

HERTZBACH
certified public accountants · consultants

www.hertzbach.com

Baltimore
800 Red Brook Boulevard
Suite 300
Owings Mills, Maryland 21117
410.363.3200

Greater Washington, D.C.
1803 Research Boulevard
Suite 215
Rockville, Maryland 20850
301.315.2150

Northern Virginia
1530 Wilson Boulevard
Suite 700
Arlington, Virginia 22209
703.351.6600

Are you ready for the new overtime rules?

In May, the Department of Labor issued new final overtime rules that update the thresholds for classifying workers as nonexempt and highly compensated. The controversial changes will increase pay for more than 4 million workers, setting the income threshold for exempt workers to the level it would have reached if the threshold hadn't been frozen more than a decade ago.

That's good news for lower- and middle-income families, but it could be costly for employers who are forced to foot the bill and implement changes to their payroll systems. Here's what you need to know to comply by the final rule's effective date of December 1, 2016.

Exempt vs. nonexempt

Under the Fair Labor Standards Act (FLSA), "nonexempt" employees must receive pay for hours worked in excess of 40 in a workweek at a rate of not less than one and a half times their regular rates of pay. In other words, a *nonexempt* worker who's regularly paid $12 an hour would earn $18 for each hour in excess of 40 in a given workweek. Who's nonexempt? The answer requires employers to apply a two-part test.

The first part is a simple income threshold. Under existing law, employees who earn less than $23,660 a year (or $455 a week) are *nonexempt* and must be paid overtime. The new rules more than double the income threshold for nonexempt workers to $47,476 a year (or $913 a week).

> Over the long run, you may decide to automate certain functions, instead of relying on human labor.

Conversely, employees who are highly compensated are automatically *exempt* from overtime pay. The current threshold for highly compensated employees of $100,000 a year will increase to $134,004 a year under the updated DOL guidance. This income threshold generally includes nondiscretionary bonuses, incentive pay and commissions that occur at least quarterly and don't exceed 10% of the employee's compensation. Both income thresholds (for nonexempt and highly compensated employees) will be adjusted every three years, starting in January 2020.

The second part of the overtime test is for employees who earn between $23,660 and $100,000 (which will increase to between $47,476 and $134,004 under the new rules). Classifying these middle-level employees as exempt vs. nonexempt depends on a duties test. Employees who "primarily perform executive, administrative or professional duties" are *exempt* and don't require overtime pay.

Critical impacts

Millions of workers will be reclassified under the new DOL rules. The results of these changes are twofold:

1. More workers earning $23,660 to $47,475 a year will be eligible for overtime pay. It doesn't matter if the worker is salaried or performs managerial or administrative duties; *nonexempt* workers below the threshold automatically qualify for overtime pay.

2. Workers earning $100,000 to $134,003 a year may also qualify for overtime pay under the new rules, depending on the type of work they perform.

These changes will affect most manufacturers. Their payroll costs will likely increase, and the changes could end flexible work arrangements that factory workers value. For example, under the new guidance, you can't allow nonexempt employees to work 45 hours one week to make up for a week in which they work only 35 hours without paying overtime pay for the workweek that exceeds 40 hours.

Legitimate ways to avoid overtime pay

Diligent employers can minimize overtime costs without violating the FLSA. For example, you can closely monitor how many hours *nonexempt* employees work and limit their hours to 40 per week. If you need extra help during peak times, you can hire temporary or part-time workers or independent contractors to fill the gaps.

Also consider giving slight raises to employees near the nonexempt and highly compensated thresholds. Doing so may actually decrease your compensation costs after you factor in the incremental costs of overtime pay. You can also cut back on benefits and perks to offset these costs.

Over the long run, you may decide to automate certain functions, instead of relying on human labor. You may have previously crunched the numbers on investing in automated equipment and decided against it, but the decision may be worth revisiting now that the cost of direct labor is rising.

NAM weighs in

Many businesses and trade organizations have responded negatively to the Department of Labor's new overtime regime. Here's what the National Association of Manufacturers (NAM) had to say about the changes when they were issued earlier this year.

"Manufacturing is a pathway to the middle class for millions of men and women who make things in America. However, this regulation creates barriers to opportunity, severely limiting flexibility and dramatically increasing red tape, especially for small manufacturers who cannot afford the burdens of a 99% salary increase for management employees who are exempt from overtime pay. Even worse, the administration has also required there to be future automatic increases, which creates uncertainty in planning in future years."

The clock is ticking

As we noted, employers must comply with the DOL's new overtime rules by December 1. If you haven't already updated payroll systems to comply with the changes, contact your tax and payroll advisors immediately. There's still time to help you comply with the FLSA, brainstorm ways to reduce (or eliminate) overtime pay and evaluate how the new rules will impact your bottom line. ■

Spotlight on fraud in the manufacturing industry

The Association of Certified Fraud Examiners (ACFE) has published its *2016 Report to the Nations on Occupational Fraud and Abuse*. The latest biennial study breaks down white collar crimes by industry, highlighting the common scams that manufacturers need to watch for and ways for them to minimize potential losses from fraud.

How much does fraud cost?

The ACFE estimates that the annual cost of fraud globally is roughly $3.7 trillion, based on a gross world product of $74.16 trillion in 2014. That's a significant amount of money, but what hits closer to home is how much fraud affects *individual* victim organizations.

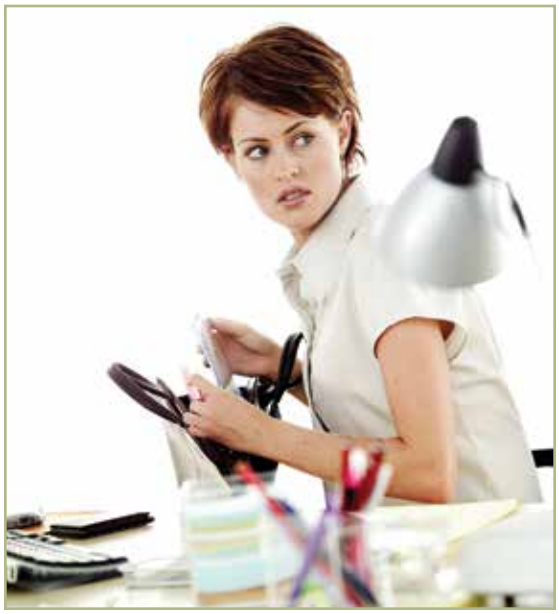
The median loss for frauds occurring at U.S. companies was $120,000, according to the 2016 report. Even more disheartening is the median loss for manufacturers of $194,000. A loss of this size would be difficult for most small manufacturers to absorb. Moreover, these estimates include only *direct* monetary losses. Fraud also potentially costs companies in terms of lost productivity, diminished employee morale and loss of confidence with customers.

Which schemes are most common?

The ACFE breaks down its findings by industry, and manufacturing ranks third in terms of the frequency of fraud cases. The most common schemes reported by manufacturers include:

Corruption. Almost half of manufacturers in the study (48.4%) fell victim to these scams. Corruption includes bribery, illegal gratuities and economic extortion.

Billing scams. About one-third of fraud cases (32.8%) involved billing ploys. These scams



may include submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.

Noncash theft. Rounding out the top three categories, noncash ploys were reported in more than 30% of fraud cases. These incidents often involve theft of such valuable assets as inventory and equipment.

In addition, roughly a quarter of fraud cases involved fictitious or exaggerated claims for expense reimbursement. Many fraudsters test the waters with these types of entry-level scams. Then they graduate to bolder schemes, if no one notices their expense fraud.

How can manufacturers fight fraud?

Fraud prevention and detection measures don't necessarily have to be expensive to be effective. According to the ACFE, the antifraud controls that offer the highest potential return on investment — that is,

offer the biggest reduction in comparative median fraud losses — include:

- Regular data monitoring and analysis techniques,
- Management review, and
- Reporting hotlines.

Across the board, the presence of antifraud controls was correlated with lower losses and quicker fraud detection. More specifically, victim organizations that were using proactive data monitoring and analysis techniques as part of their antifraud program suffered fraud losses that were 54% lower and detected the frauds in half the time compared to organizations that didn't use these techniques. Management review and the presence of a hotline were correlated with 50% lower median losses and 50% less time to detect the scheme.

How should victims handle fraud allegations?

The majority of the fraud victims in the ACFE study haven't yet recovered a dime from the perpetrators. Many worry that prosecuting criminals could lead to bad publicity. Others prefer to just fire the wrongdoers and then focus on recovery, rather than spend time and resources pursuing a financial settlement or conviction.

Prosecuting fraud may be worthwhile for several reasons, however. It sends a message to would-be thieves that management has adopted a zero-tolerance policy, thereby deterring future crimes. In addition, a conviction will be reported on the fraudster's permanent record, which may prevent him or her from striking other victims in the future. If you suspect fraud, contact your attorney or a forensic accountant for help deciding how to proceed. ■

Understanding tax issues related to shareholder loans

Owners occasionally borrow funds from their businesses. You may, for example, need an advance to cover your child's college costs or a down payment on a vacation home. If your company has extra cash on hand, a shareholder loan can be a convenient and low-cost option — but it's important to treat the transaction as a bona fide loan. If you don't, the IRS may claim the shareholder received a taxable dividend or compensation payment rather than a loan. Here's more information to protect shareholder advances from IRS scrutiny.

A closer look at AFRs

You can make de minimis loans of $10,000 or less to shareholders without paying interest. But, if all

of the loans from the business to a shareholder add up to more than $10,000, the advances may be subject to a complicated set of below-market interest rules *unless* you charge what the IRS considers

an "adequate" rate of interest. Each month the IRS publishes its applicable federal rates (AFRs), which vary depending on the term of the loan.

Right now, interest rates are near historical lows, making it a good time to borrow money. For example, in July 2016, the adjusted AFR for short-term loans (of not more than three years) was only 0.65%. The rate increased to 1.16% for mid-term loans (with terms ranging from three years to not more than nine years). Both rates are probably below what a bank would charge. As long as the company charged interest at the AFR (or higher), the loan would be exempt from the complicated below-market interest rules the IRS imposes.

The interest rate for a demand loan — which is payable whenever the company wants to collect it — isn't fixed when the loan is set up. Instead it varies depending on market conditions. So, calculating the correct AFR for a demand loan is more complicated than it is for a term loan. In general, it's easier to administer a shareholder loan with a prescribed term than a demand note.

Below-market loans

If your company lends money to an owner at an interest rate that's below the AFR, the IRS requires it to impute interest under the below-market interest rules. These calculations can be complicated. The amount of incremental imputed interest (beyond what the company already charges the shareholder) depends on when the loan was set up and whether it's a demand or term loan.

Additionally, the IRS may argue that the loan should be reclassified as either a dividend or additional compensation. The company may deduct the latter, but it will also be subject to payroll taxes. Both dividends and additional compensation would be taxable income to the shareholder personally, however.

Bona fide loans

When deciding whether payments made to shareholders qualify as bona fide loans, the IRS considers:

- The size of the loan,
- The company's earnings and dividend-paying history,
- Provisions in the shareholders' agreement about limits on amounts that can be advanced to owners,
- Loan repayment history,
- The shareholder's ability to repay the loan, based on his or her annual compensation, and
- The shareholder's level of control over the company's decision making.

The IRS will also factor in whether you've executed a formal, written note that specifies all of the repayment terms. The loan contract should spell out such details as the interest rate, a maturity date, any collateral pledged to secure the loan and a repayment schedule.

Getting started

If you'd like to take advantage of today's low interest rates, a shareholder loan could be a smart tax planning move to make this year. Contact your tax advisor for more information. He or she can help set up and monitor your shareholder loans to ensure compliance with the IRS rules. ■

Cyberrisks mount

Preventive measures for manufacturers

Cyberattacks are on the rise. Manufacturers who rely on automation, robotics and connected networks are especially vulnerable. Here's what you can do to protect your business against ransomware and other attacks from criminals using the Internet of Things.

Know your risks

Last December, hackers caused a blackout in the Ukraine by breaching the control system for a power grid. This attack didn't require sophisticated tools; rather, the hackers used malware that could be purchased on the black market to engage in spear phishing. This is a type of email phishing campaign that targets multiple people at an organization using inside information that makes the hacker's inquiry look legitimate.

Owners and managers fear data breaches — and hackers often use that fear to cripple organizations through ransomware. This is a type of malware that's installed on a computer or network without the user's consent that relinquishes control back to management only if they agree to pay ransom to the malware operators. Once the money is paid, the hackers promise to remove the restrictions.

Cyberattacks can harm a manufacturer or distributor by causing safety issues, negative publicity, lost productivity, and compromised personal and corporate data. The average cost of a data breach in the United States is now more than $7 million, according to a 2016 study published by independent research group The Ponemon Institute.

Safeguard your operations

How can you reduce cyberrisks? Employees are a manufacturer's first line of defense against hackers, but they can also be a liability if they're not vigilant and knowledgeable about cyberthreats. In fact, the latest Ponemon study found that 23% of breaches were caused by negligent employees. So, it's critical to provide training about the latest scams and encourage employees to report suspicious emails immediately to the information technology department.

Many hackers look for easy targets — like thieves target houses with unlocked doors and windows to break into — so even the simplest security measure will deter some cyberbreaches. For example, you can use inexpensive, over-the-counter encryption software and phishing filters to make it harder for hackers to get inside your network.

Reduce losses

To minimize losses if a breach occurs, consider purchasing cyberinsurance products to cover direct losses from breaches and the costs of responding to them. Your traditional business liability policy probably doesn't include such coverage.

You can also assemble a breach response team *before* a breach occurs. Doing so decreases the average cost of a data breach by about 12%, according to the Ponemon study. Once it's formed, the response team can also identify potential weaknesses in your network and conduct breach response drills. ■

HERTZBACH
certified public accountants · consultants

800 Red Brook Boulevard
Suite 300
Owings Mills, MD 21117

Serving the **manufacturing industry** for over 65 years.

We provide the tools to **improve your bottom line.**

TAX & ASSURANCE
- Cost Allocations and Inventory
- Product Valuation
- Federal and State Tax Filings
- Multi-State Tax Issues
- Tax Credits such as R&D, Employment & Property
- UNICAP Costing
- Overall Tax "Check Up"
- Research Client Questions
- Representation Before IRS and State Examiners

CONSULTING
- Strategic Planning
- Cash Management
- Budget Preparation
- Information Technology Systems & Implementation
- Forecasts & Projections
- Lease vs. Purchase Analysis
- Performance Measurement
- Insurable Risk Management & Analysis of Potential Exposure
- Policies and Procedures Manuals

HERTZBACH
certified public accountants · consultants

800.899.3633
www.hertzbach.com
manufacturing@hertzbach.com