Robinson+Cole

Manufacturing Law Blog

Recent Posts - Hot Topics + Issues

FROM WWW.MANUFACTURINGLAWBLOG.COM

Jeff White
Partner, Chair
Manufacturing Law Group
jwhite@rc.com

Edward Heath
Partner, Chair
Business Litigation Group
eheath@rc.com

Five Tips for Managing Internal Emails in Supply Chain/Customers Disputes

AUTHORED BY JEFFREY WHITE ON AUGUST 10, 2021

In the past, we have provided some guidance about how to manage supply chain and other business to business disputes.

2020-2021 has been the year of supply chain disruptions and customer disputes. Not all disputes lead to a courtroom – many of them are resolved. However, there are certain practices when it comes to sending internal emails that are worthwhile to consider. Some of these are obvious.

1. A lot of times when we talk about email practices, we look at it defensively, i.e., if there is a dispute. Some of my partners call email "God's gift to trial lawyers." I think the point they are making is that email can be misconstrued because typically "tone" is read in and also because it often is written quickly. So, as an initial rule, I encourage people to apply the 24 hour rule if the email is dispute oriented at all. Sometimes you can't wait to respond, but if you can, it is always better to send a placeholder email.
2. Avoid sarcasm or jokes because again, it often is not delivered the right way.
3. Mind your cc's. Ccs are often used as a weapon and when dealing with a customer/supplier/vendor, it can look like you are taking someone to the "principal's office." Also, there may be a strategic reason to keep executive management out of it until the right time.
4. For smaller companies, you should encourage people to relay significant concerns in person or over the phone. On the quality side, I know a lot of folks want to email the world, but oftentimes I have seen engineers, etc. speculate about issues and then change their minds. But, that initial email is there forever. So, make sure folks adequately investigate something before putting it in writing.
5. When we train quality/sales, etc. we always tell people that emailing people is fine. Often, when you give people rules, they say they will never email anyone again. It is more about helping them identify the risks themselves as opposed to telling them what to do.

Robinson+Cole

Manufacturing Law Blog

Recent Posts - Hot Topics + Issues

FROM WWW.MANUFACTURINGLAWBLOG.COM

What The EEOC Says About Requiring Vaccines at Work

AUTHORED BY ABBY WARREN, ALISHA SULLIVAN AND EMILY ZAKLUKIEWICZ ON JULY 26, 2021

For many months, manufacturers have been navigating issues related to the COVID-19 vaccine and its impact on the workplace. This includes implementation of vaccination programs that require or encourage vaccination of frontline workers, who remain at a higher risk of COVID-19 exposure and infection.

Manufacturers have been tasked with remaining up to date on relevant legal obligations and practical considerations surrounding vaccination policies, incentive programs, reasonable accommodations, employee relations and communications, among other issues. In late May, the Equal Employment Opportunity Commission (EEOC) updated its technical-assistance guidance for the first time since December 16, 2020, clarifying several important topics related to workplace vaccination programs. **Read the article.**

OSHA Publishes Updated COVID-19 Guidance

AUTHORED BY MEGAN BARONI ON JUNE 24,2021

Thank you to **Jonathan Schaefer** for his contributions to this post. Jon focuses his practice on environmental compliance counseling, occupational health and safety, permitting, site remediation, and litigation related to federal and state regulatory programs.

On June 21, 2021, OSHA made big news by publishing its COVID-19 **Emergency Temporary Standard** for the Healthcare Industry (ETS). While the ETS does not apply to most manufacturing facilities, OSHA also updated its general COVID-19 **guidance** earlier this month.

This guidance is intended to assist all employers and workers not subject to the ETS in mitigating the spread of COVID-19. The main recommendations in the guidance are summarized below:

- Workplaces with Fully Vaccinated Employees. Employers no longer need to take as many steps to protect fully vaccinated employees from COVID-19. However, unvaccinated or at-risk workers still need to be protected. As such, employers are strongly advised to support their employees in getting vaccinated by granting them paid time off to receive the vaccine and paid time off to recover from any of vaccine side effects.

- Protecting Unvaccinated or At-Risk Employees:

    - Work from home. Any COVID-19 infected workers, or ones who have had close contact with someone who tested positive for COVID-19, should work from home, or receive paid time off as needed.
    - Physical distancing. Unvaccinated and at-risk workers should maintain a 6 feet distance from others, or be separated at fixed workstations behind transparent shields or other solid barriers.
    - Facemasks. Employers should provide facemasks at no cost for their unvaccinated and at-risk workers. Employers should also suggest that unvaccinated visitors wear facemasks in the workplace.

- Other workplace safety guidelines:
    - Educating Employees on COVID-19. Managers should be trained on COVID-19 transmission risks and be frequently updated on any workplace COVID-19 policies. Employees should also be informed of their rights to protection against COVID-19 in the workplace.
    - Ventilation Systems. Employers should maintain adequate ventilation systems. Air filters with a Minimum Efficiency Reporting Value (MERV) 13 or higher should be installed where feasible.
    - Cleaning and disinfection. If someone who has been in the facility within 24 hours is suspected of having or confirmed to have COVID-19, the **CDC cleaning and disinfection recommendations** should be followed.
    - Record and report. Employers are responsible for recording work-related cases of COVID-19 illness on Form 300 logs. Employers must also follow regulatory requirements when **reporting COVID-19 fatalities and hospitalizations to OSHA.**
    - Retaliation. No employees should be discharged or discriminated against for raising a reasonable concern about workplace COVID-19 infection, or exercising any of their rights under the COVID-19 policies and procedures.
    - Other applicable mandatory OSHA standards. All of OSHA's standards that apply to protecting workers from infection remain in place. These mandatory OSHA standards include: requirements for personal protective equipment, respiratory protection, sanitation, protection from bloodborne pathogens, OSHA's requirements for employee access to medical and exposure records and, of course, the General Duty Clause.

Prometheus Ransomware Targeting Manufacturing Sector

AUTHORED BY LINN FREEDMAN ON JUNE 15, 2021

Since the Colonial Pipeline and JBS meat manufacturing security incidents, attention is finally being paid to the cybersecurity vulnerabilities of critical infrastructure in the U.S. and in particular, the potential effect on day to day life and national security if large and significant manufacturers' production are disrupted. In the wake of these recent incidents in the manufacturing sector, Unit 42 of Palo Alto Networks has published research that may be considered a warning to the manufacturing sector and is worth notice. The warning is about the activities of Prometheus, "a new player in the ransomware world that uses similar malware and tactics to ransomware veteran Thanos."

According to the Executive Summary, Unit 42 "has spent the past four months following the activities of Prometheus" which "leverages double-extortion tactics and hosts a leak site, where it names new victims and posts stolen data available for purchase." Prometheus claims to be part of REvil, but Unit 42 says it has "seen no indication that these two ransomware groups are related in any way." Unit 42 further states that Prometheus claims to have victimized 30 organizations in different industries, in more than a dozen countries, including the U.S.

Prometheus came on the scene in February 2021 as a new variant of the strain Thanos. Unit 42 is unable to provide information on how the Prometheus ransomware is being delivered, but surmise that it is through typical means, such as "buying access to certain networks, brute-forcing credentials or spear phishing for initial access." It then first kills backups and security processes and enables the encryption process. It then "drops two ransom notes" that contain the same information about the fact that the network has been hacked and important files encrypted and instructions of how to recover them. If the ransom demand is not met, the data will be published on a

shaming site and publishes the "leak status" of each victim. According to Unit 42 "[M]anufacturing was the most impacted industry among the victim organizations we observed, closely followed by the transportation and logistics industry."

What we have seen in the past is that when ransomware groups are successful in one industry, they use the information learned from initial attacks to target other companies in that sector. They leverage the knowledge from one attack to future attacks assuming that since the first one was successful, subsequent attacks will be successful as well. Since industry specific networks are similar, it is seamless to attack one victim, learn from it, then leverage that knowledge to attack similarly situated victims.

With threat attackers' focus on the manufacturing sector right now, we anticipate seeing more attacks against manufacturers from groups such as Prometheus.

Alleged Aerospace Export Violations by Honeywell Lead to $13 million Settlement Following Voluntary Self-Disclosure

AUTHORED BY EDWARD HEATH AND KEVIN DALY ON JUNE 15, 2021

Earlier this month, it was announced that Honeywell International, Inc. (Honeywell) had entered into a $13 million administrative settlement with the U.S. government to resolve allegations of export control violations related to aerospace and defense technical data (specifically engineering prints for castings and parts for aircraft, gas turbine engines, and military electronics). Following a self-disclosure by Honeywell to the federal government, the State Department alleged that the company committed 34 violations of the Arms Export Control Act (AECA) and International Traffic in Arms Regulations (ITAR) in connection with data exported to recipients in Canada, Mexico, Ireland, China, and Taiwan without required government approval.

The most significant takeaway from this settlement is the leniency that Honeywell earned by virtue of its self-disclosure, cooperation with the State Department's follow-up inquiries, and prompt self-policing. First, because maximum civil penalties for these alleged AECA and ITAR violations are just over $1.1 million per violation, Honeywell would have faced over $37.4 million in aggregate civil penalties based upon the allegations. Second, the government cited the voluntary disclosure as a reason that it did not seek to debar Honeywell from participation in government programs. Finally, the government agreed that $5 million of the $13 million settlement payment is suspended on the condition that Honeywell uses that amount to fund the compliance upgrades prescribed by the settlement agreement.

While any potential self-disclosure of suspected international trade compliance violations requires careful and thoughtful analysis, this latest AECA/ITAR settlement suggests that the Biden Administration may place significant value on corporate candor and cooperation.