



PROGRAM MATERIALS

Program #30114

May 28, 2020

Key Workplace Considerations as We Enter the New Normal: COVID-19 Implications Today, Tomorrow and Beyond

**Copyright ©2020 by Mara Levin, Esq., Caroline Powell
Donelan, Esq. and Stephanie Kaplan, Esq. - Blank Rome
LLP.**

All Rights Reserved.

Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center

www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487

Phone 561-241-1919

Fax 561-241-1969

Key Workplace Considerations As We Enter the New Normal:
**COVID-19 Implications Today,
Tomorrow and Beyond**

Caroline Powell Donelan
Stephanie Gantman Kaplan
Mara B. Levin

May 28, 2020

Mandatory Disclaimer...

© 2020 Blank Rome LLP

The purpose of this CLE is to identify select compliance issues that may be of interest to participants. The information contained herein is abridged and summarized from various sources, the accuracy and completeness of which cannot be assured. This update is not and should not be construed as legal advice or opinion, and is not a substitute for the advice of counsel.

BLANKROME

Today's Presenters:



Caroline Powell Donelan
Partner
Los Angeles
Labor & Employment
424.239.3476
cdonelan@blankrome.com



Stephanie Gantman Kaplan
Partner
Philadelphia
Labor & Employment
215.569.5381
sgkaplan@blankrome.com



Mara B. Levin
Partner
New York
Labor & Employment
212.885.5292
mlevin@blankrome.com

BLANKROME

Compliance Matters

“Everybody has a plan until they get punched in the mouth”
- Mike Tyson



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

BLANKROME

Agenda

- ***Today...***
 - Layoffs and Furloughs
 - Federal and State WARN Considerations
 - FFCRA and other Leave Issues
- ***...Tomorrow***
 - Health Screenings and Privacy Considerations
 - Reasonable Accommodations under the ADA
 - Safety Protocols
- ***...and Beyond***
 - A **Greener** World
 - Redesigned Office Configurations
 - Technological Impact of Remote Working



COVID-19 Implications Today:

Weighing Layoffs vs. Furloughs to Mitigate COVID Losses

- Layoffs

- Generally recommended when employer is uncertain of how long employees will need to stay out of work.
- Laid off employees are terminated, so state-specific final pay rules apply (timing, payout of accrued PTO, etc.)
- Laid off employees should be provided information on unemployment insurance benefits and COBRA continuation coverage.

- Furloughs

- Generally recommended as a short term response to slow business when there is some certainty as to when employees will be recalled – e.g., furlough will last for 2-3 weeks and employer wants to retain workforce and continue group benefits.
- Unclear whether long term furloughs trigger final pay rules, which are state specific. If available, furloughed employees should be provided anticipated return to work dates (even if subject to change) and clear communications regarding benefits, available paid time off, and regular updates to support an ongoing employment relationship.
- Group health benefits during a furlough are plan dependent; if there are minimum hours required under the plan that are not met because of a furlough, the furlough could become COBRA-qualifying event and COBRA continuation should be offered.
- Some states allowed furloughed employees or those with reduced hours to receive state unemployment benefits even if they do not meet standard eligibility requirements; also may be eligible under the CARES Act.
- Generally, employers do not need to pay non-exempt employees for time not worked. However, if an exempt employee performs *any* work during a given workweek, the employee generally must receive their entire salary for that week.
- Employers should clearly communicate, expect and prepare for the fact that furloughed employees will not work during certain periods of time, including checking email and voicemail. Inform all employees in writing that work is not authorized during the furlough period (without advance written approval).

Federal WARN Act: Plant Closing v. Mass v. Layoff

Under the Federal WARN Act, employers with 100+ employees must provide at least **60 days' advance, written notice** prior to any "mass layoffs" or "plant closings," defined as...

Plant Closing	Mass Layoff
A permanent or temporary shutdown of a single site of employment that results in an " <u>employment loss</u> " for 50 or more employees in any 30-day period. Employment loss is: (a) a termination, other than for cause; (b) a layoff exceeding 6 months; or (c) a reduction in work hours of more than 50% in each month of any 6 month period.	A reduction in force that is not the result of a plant closing and that results in an employment loss at a single site of employment during any 30-day period for: (a) at least 33% of full-time employees and at least 50 or more full time employees; <i>or</i> (b) at least 500 full-time employees.



BLANKROME

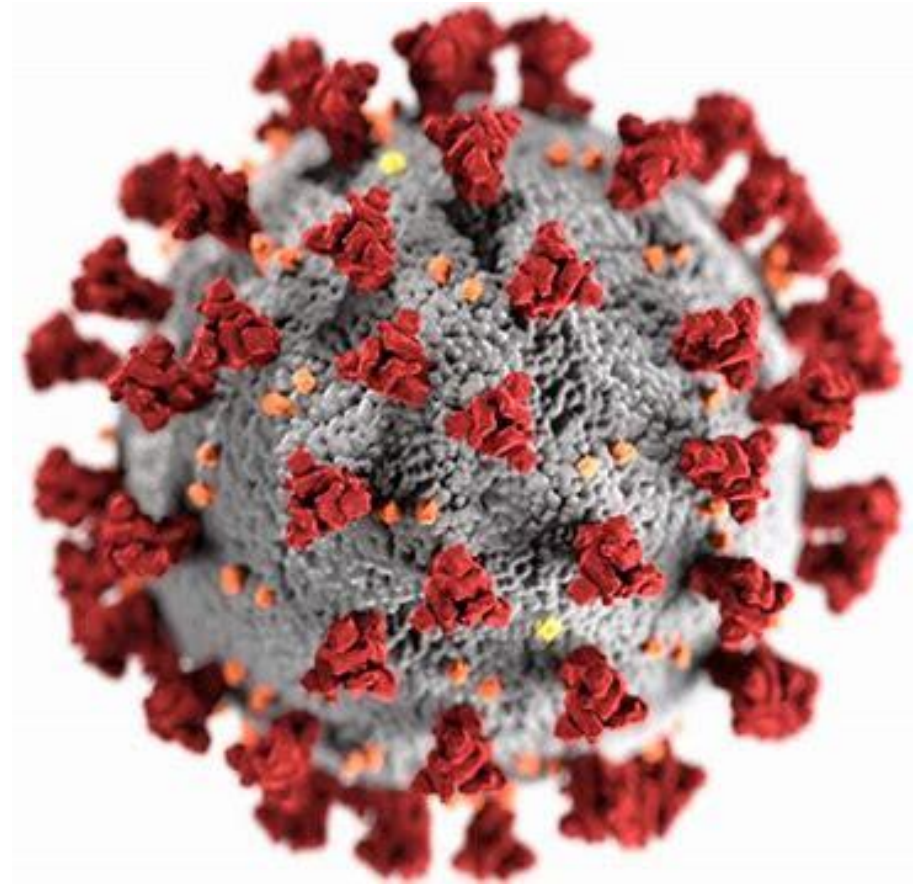
Do Layoffs and Furloughs Trigger the Federal WARN Act?



- ✓ Covered employer (100+)?
- ✓ Plant Closing (“employment loss” of 50+ within 30 day period)?
- ✓ Mass Layoff (33% and 50+ FT *or* 500+ FT, each in 30 day period)?
- ✓ Duration (6 months or more)?

Federal Exceptions to WARN Notice Requirements

- **“Faltering Company”** - This exception applies when, before a plant closing, a company is actively seeking capital or business and reasonably in good faith believes that advance notice would preclude its ability to obtain such capital or business, and this new capital or business would allow the employer to avoid or postpone a shutdown for a reasonable period.
- **“Unforeseeable Business Circumstances”** – This exception applies when the plant closing or mass layoff is caused by business circumstances that were not reasonably foreseeable at the time that 60-day notice would have been required.
- **“Natural Disaster”** – This exception applies when a plant closing or mass layoff is the direct result of a natural disaster such as a flood, earthquake, drought, storm, tidal wave, or similar effects of nature. In this case, notice may be given after the event.



Is COVID-19 an “unforeseeable business circumstance” for purposes of the federal WARN Act?

- Very likely that the COVID-19 pandemic and its significant economic effects will be considered an “unforeseeable business circumstance.”
- Even so, this exception does not eliminate an employer's obligation to notify affected employees and certain state and local officials **as soon as practicable**.
- Also, as we move deeper into the pandemic, now months in, it will be more challenging to support this “unforeseeable business circumstance” standard.
- Again, state laws also vary, and many do not provide for this exception.



BLANKROME

State Mini WARN Laws



- Many states have “mini-WARN Act” statutes and related laws, including California, Delaware, Hawaii, Illinois, New York, New Jersey, Maine, Michigan, Ohio, Maryland, and Massachusetts.
- State law is often more protective of workers than the federal WARN Act, and differs from the federal Act with respect to triggering events, exceptions, employee threshold counts, as well as notice content and required recipients.

Families First Coronavirus Response Act: “FFCRA 101”

- Effective Dates: **April 1, 2020 – December 31, 2020**
- Employee Notice Required - posting FAQ's online
- “Covered Employer” = those with *fewer than* 500 employees
 - *Count done at time of leave – include all employees within U.S., exclude only contractors and furloughed/ laid off staff*
 - *There is only a partial exemption for employers with fewer than 50 employees; not a blanket “small business” exemption.*
- Creates two new paid leave entitlements created: (1) emergency paid sick leave; and (2) emergency paid family leave (amends the FMLA)
- Laid off/ furloughed employees are not entitled to paid sick or expanded family leave under the FFCRA
- 100% reimbursed through tax credits with proper documentation



BLANKROME

Back to Basics: “FFCRA 101”

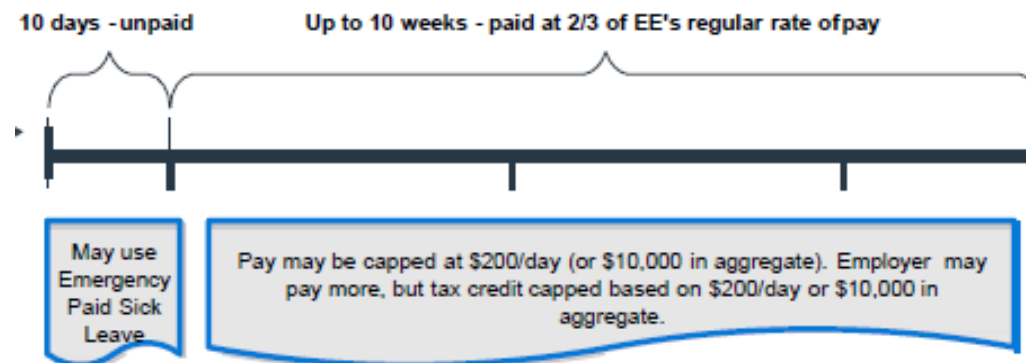
#1 Emergency Paid Sick Leave (“EPSL”): Gives all employees up to 80 hours (10 workdays) of emergency paid sick leave for:

1. Their own quarantine or isolation order under federal, state or local law;
 2. To self-quarantine, as advised by a health care provider;
 3. Because they are experiencing symptoms and seeking a medical diagnosis;
 4. To care for another individual subject to a quarantine or isolation order or advised to self-quarantine (not limited to family members);
 5. To care for a child as the result the child’s school closing or the closing or unavailability of the childcare provider; or
 6. Because the employee is experiencing any other substantially similar conditions specified by the Secretary of Health and Human Services, in consultation with the Secretaries of Labor and Treasury.
- Nos. 1-3 paid at 100% of regular rate (subject to caps)
 - Nos. 4-6 paid at 2/3 regular rate (subject to caps)

Back to Basics: “FFCRA 101”

#2 Emergency Paid Family Leave (“EPFL”)

- For reason No. 5 (“to care for a child as the result the child’s school closing or the closing or unavailability of the childcare provider”), employees may also qualify for up to 12 weeks of job-protected emergency family leave.
- If so, EPSL runs *concurrently* with, and counts toward, the total 12 weeks available for EPFL:



Back to Basics: “FFCRA 101”

- **Limits on Compensation Are Based on the Underlying Qualified Reason for the Leave:**
 - \$511 per day and \$5,110 in the aggregate for sick leave for reasons (1)-(3)
 - \$200 per day and \$2,000 in the aggregate for sick leave for reasons (4)-(6)
 - \$200 per day and \$10,000 in the aggregate for paid family and medical leave for reasons described in (5)
- **Employers are entitled to a fully refundable tax credit equal to the paid leave required,** plus allocable qualified health plan expenses and the employer’s share of Medicare tax.
- Employers can retain federal employment taxes equal to the amount of FFCRA leave paid, plus qualified health plan expenses and the employer’s share of Medicare tax imposed on those wages, rather than depositing them with the IRS.

Back to Basics: “FFCRA 101”

- “Protected” means employees have a right to reinstatement to the “same or equivalent” job.
- Group health coverage (if any) continues during leave.
- Employees may (*but do not have to*) supplement EPSL with existing PTO.
- Employees may (*and can be required to*) supplement EPFL with existing PTO.
- Documentation is key to: (1) prevent abuse; and (2) ensure reimbursement
 - ✓ Reason for leave and statement from employee that he/she unable to work
 - ✓ Name of healthcare provider
 - ✓ Copy of quarantine order
 - ✓ Copy of email from school/ childcare provider regarding closure

FFCRA Posting Requirements

DOL Has Published 14 “Posting FAQ’s” online:

<https://www.dol.gov/agencies/whd/pandemic/ffcra-poster-questions>

- ✓ Email/ Mail
- ✓ Intranet
- ✓ Worksite

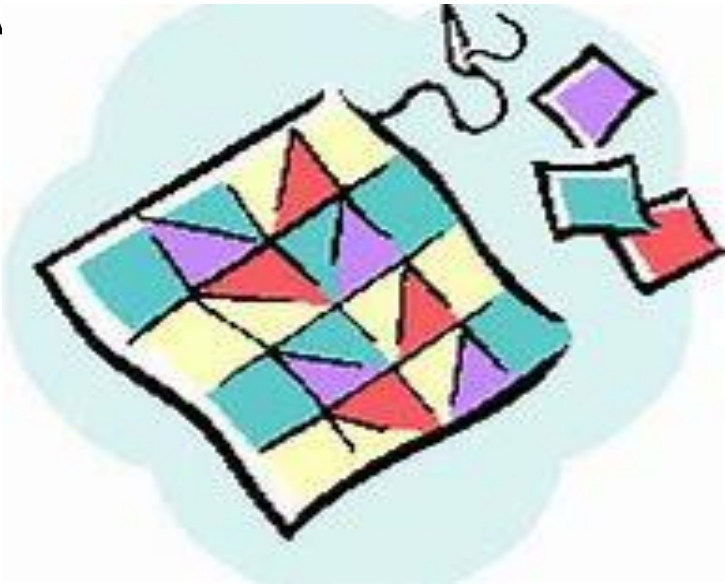


BLANKROME

Other Leave Considerations – Navigating the Patchwork

Federal Leave Rights

- FMLA
- FFCRA
- ADA

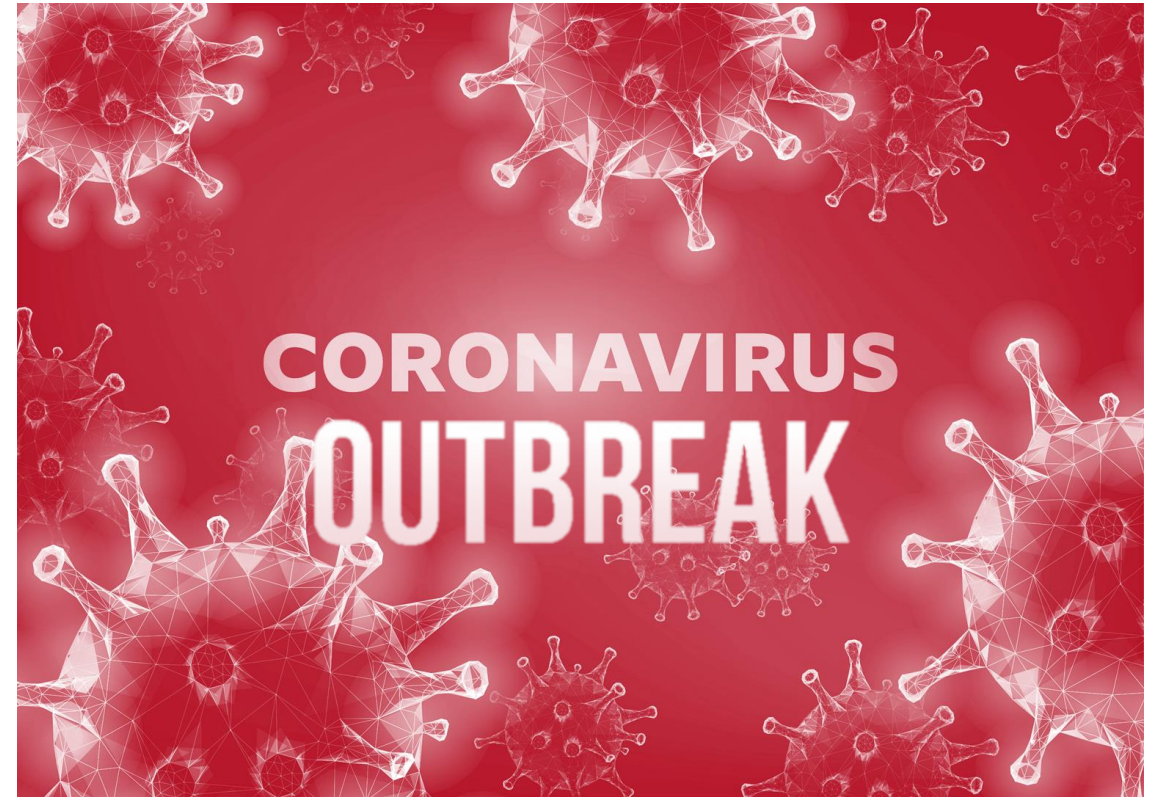


State and Local Leave Rights

- Traditional or Supplemental Paid Sick Leave (Local and State)
- State Local and Family Medical Leaves
- Child Care Leaves
- State Disability Leaves

Operating Assumption Should Be That *Everyone* In Your Workforce Will Take FFRCA or Some Other Protected Leave This Year

- More than 1,000,000 confirmed COVID-19 cases in the U.S.; nearly 100k deaths.
- Over 90% of the world's student population is currently affected by school closures.
- 46 states are under some kind of shutdown order.



Operating Assumption Should Be That *Everyone* In Your Workforce That Is Eligible May Take Some Type of Leave This Year

- Assign and equip your “Leave Team” – HR, Payroll, Tax, Finance
- Decide core functions and build redundancies in key positions
- Properly manage communications
- Plan for monitoring legal changes, but do not “Panic React” to every breaking development



Making Sure You Get and Keep The Documentation You Need For Reimbursement

- Documentation is mandatory for reimbursement (4 year retention)
- Build all the information you need and are permitted to obtain right into your FFCRA request form:



REQUEST FOR EMERGENCY FAMILY AND MEDICAL AND/OR PAID SICK LEAVE

Employees requesting Emergency FMLA (EFMLA) or Emergency Paid Sick Leave (EPSL) under the Families First Coronavirus Response Act (FFCRA) must complete this form in its entirety and submit it to **Human Resources** via **Email/Intranet Site**. Leave is only available between April 1, 2020 and December 31, 2020 unless otherwise extended by law.

Employee Name: _____

Employee Home Address: _____ **E-mail:** _____

Home Phone Number: _____ **Cell Phone Number:** _____

This is a (choose one): ☐ New request for leave ☐ Request for an extension of leave

Anticipated Start Date of Leave: _____ **Expected Return to Work Date:** _____

Reason for Leave (check all applicable): I am unable to work or telework for the following reasons:

☐ I am subject to a federal, state, or local quarantine or isolation order. (List the name of government entity that issued the quarantine or isolation order): _____

☐ I have been advised by a health care provider to self-quarantine. (List the name of healthcare professional advising self-quarantine): _____

☐ I am experiencing symptoms of COVID-19 and seeking a medical diagnosis.

☐ I am caring for an individual that is subject to a federal, state, or local quarantine or isolation order or has been advised by a health care provider to self-quarantine. (List the name of the individual and relation of individual to you and of the government entity issuing the order/of the individual's healthcare provider): _____

☐ I am caring for my son or daughter under age 18 (or 18 or over if disabled and cannot care for self) because his/her school or place of care has been closed, or his/her childcare provider is unavailable, due to COVID-19 precautions. (List the name and age of the child/children to be cared for, the name of the school/place of care): _____

COVID-19 Litigation – What We Have Seen and Learned *Already*



- For most claims, including FFCRA, there are no administrative hoops; claims can go directly to the WHD or court.
- Employees are ready and willing to file.
- Individuals can sometimes face personal liability (including under the FFCRA).
- Available remedies make claims appealing to plaintiffs' bar:
 - ✓ Unpaid leave payments
 - ✓ Liquidated damages
 - ✓ Attorneys' fees



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

DOL FFCRA Questions and Answers

Last Updated May 7, 2020

<https://www.dol.gov/agencies/whd/pandemic/ffcra-questions>

BLANKROME

Covid-19 Implications Tomorrow: Return to Work Issues

What actually is a Return to Work?

- Reopening after shutdown
- Recalling furloughed, laid off and/or remote employees
- Resuming “normal” business activities

What should companies be doing?

- Reviewing applicable federal, state and local orders and guidelines to develop a compliant plan
 - CDC: <https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/businesses-employers.html>
 - OSHA: <https://www.osha.gov/SLTC/covid-19/>
- Updating policies and drafting protocols
- Communicating with the workforce



BLANKROME

Government Guidance & Reopening Requirements

“Opening Up America Again”

- Broad non-binding federal guidelines
- Employers should “[d]evelop and implement appropriate policies, in accordance with Federal, State, and local regulations and guidance, and informed by industry best practices.”

State Reopening Orders

- Detailed binding and advisory guidance
- Shutdown risk for non-compliance



BLANKROME

Consider Employee Health Screening & Testing

- Health Screening Questionnaires
 - Low cost, non-invasive, and respectful of employee privacy
 - Reliant self-assessment and employees may not recognize or report symptoms
- Temperature Screening
 - Contact (i.e. forehead) vs. Touchless (i.e. thermal or infrared) vs. Self-Check/Report
 - Training, privacy, cost, and other considerations
 - What about asymptomatic cases?
 - Required in some states for all employees or after COVID-19 positive employee at work, recommended in others
- Covid-19 Testing
 - Viral vs. Antibody Testing
 - Availability, accuracy, and retesting considerations
- Privacy Considerations
 - EEOC Guidance: Screening permitted even though generally medical exam (<https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws>)
 - Confidentiality of medical information under ADA, FMLA, state laws



BLANKROME

Temperature Screening Best Practices

- Coordinate with building management, if applicable
- Scan all employees and visitors
- Use touchless or automatic scanning technology
- Six-foot distancing in waiting area
- Ensure personnel are trained and have PPE
- Respect and maintain employee privacy
- 100.4 degrees F – CDC threshold
- Compensate non-exempt employees for screening time in accordance with the FLSA and state wage & hour laws
- ***Not all Covid-19 cases have fevers and not all fevers are Covid-19***



BLANKROME

Developing Safety Protocols

- Reassess current practices with focus on protecting employee health and safety
- Examples include:
 - Masks, gloves, and other PPE
 - Employee transportation/travel (parking subsidies to avoid transit?)
 - Elevator usage (limited occupancy/social distancing)
 - Shared workspaces (suspend or modify use?)
 - Mail and packages (no-contact delivery)
 - Hand washing or sanitizing (mandatory breaks?)
 - Special protocols for retail/customer areas




COVID-19
Novel Coronavirus


Help prevent the spread of germs and protect yourself from COVID-19 and other respiratory viruses.

Social Distancing on Elevators

2 metres apart




No more than three people



- Keep 2 metres apart from others
- There should not be more than three people per elevator

Visit toronto.ca/covid19

 **Toronto**

BLANKROME

Changes to the Workplace – Considering a New Normal

- Workplaces will require adjustment to ensure social distancing
- Plan for a sustainable “new normal”
- Some specific considerations:
 - Rearrange and modify desks, cubicles, and workstations
 - Consider repurposing conference and break rooms
 - Designate six-foot distances around workstations and other gathering spaces (copiers, printers, kitchen areas etc.)
 - Mark hallways for one-way foot traffic
 - Adjust seating in communal areas and conference rooms that remain open
- Don't forget less obvious spaces – restrooms, file rooms, break room



BLANKROME

Employer Protocols: What To Do When Employees Get Sick

Contact Tracing

- A core disease control measure employed by local and state health department personnel for decades, is a key strategy for preventing further spread of COVID-19.
 - <https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html>

Employee Communication

- Advise those in close (less than 6 feet) and prolonged (15 minutes) contact – per CDC current guidelines <https://www.cdc.gov/coronavirus/2019-ncov/php/public-health-recommendations.html>
- Consider advising entire location

CDC Guidance:

Advise infected employee when can return to work in accordance with current CDC guidance: <https://www.cdc.gov/coronavirus/2019-ncov/hcp/disposition-in-home-patients.html>

Americans with Disabilities Act (“ADA”): Reasonable Accommodations

The ADA requires that employers engage in the interactive process with qualified individuals with disabilities to provide reasonable accommodation(s) so that they can perform their essential job function.

- *UNLESS* the accommodation will pose a direct threat to the health or safety of other individuals in the workplace *or* cause an undue burden

What is a “disability” under the ADA?

- Physical or mental impairment that substantially limits a major life activity;
- A record of such an impairment; or
- Being regarded as having such an impairment

What is a “reasonable accommodation”?

- Adjustments to work environment, or manner/circumstances under which the job (or application) is customarily performed
- Can include job restructuring; part-time or modified work schedules; reassignment to a vacant position; equipment or devices; obtaining readers or interpreters; extending leave; or other similar accommodations
- Analyzed on an individualized case by case basis

What are reasonable accommodations employers can anticipate in the wake of COVID-19?

- Exemptions from wearing PPE
- Telecommuting

BLANKROME

Policy and Travel Considerations



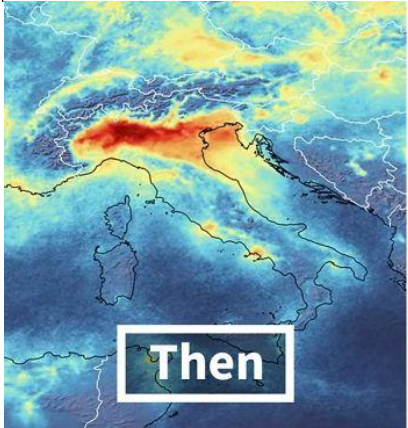
- Companies should review current policies and procedures and consider updates for legal compliance and new practices
- For companies with travel for work - review state orders of locations where employees will travel to/from
 - Some states require immediate 14 day quarantine if traveler is coming from an area with a lot of infections
 - Travelers must abide by orders of where they are traveling
 - Consider requiring employees to report travel (personal and business) to the company
 - This determination may vary depending on if employees come to the office, and if the office is located in an area with a high concentration of cases
 - Consider ban on international travel
 - CDC guidance on travel related exposure:
<https://www.cdc.gov/coronavirus/2019-ncov/php/risk-assessment.html>

BLANKROME

COVID-19 Implications Beyond



Reduce Emissions



BLANKROME

COVID-19 Implications Beyond: How Will Society Change?

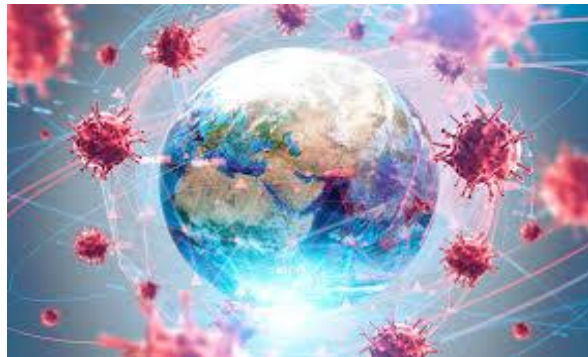
What have we learned from History?



Protests that led to OSHA as well as additional safety standards



Triangle Shirtwaist Factory Fire, 1911



What changes will Covid-19 bring to our working environment?



Women enter the workplace in great numbers leading to equal pay

BLANKROME

Remote Work: The New Normal For Years to Come

U.S. Employment Stats:

In March 2020: 130 million workers in U.S.

In April 2020: 113.66 million workers in U.S.

Pre-Pandemic

- 400% rise in remote work from 2010 to 2019
- 4.7 million working remotely in 2019

Upon U.S. lockdown:

- 16 million working remotely
 - 78% work from home
 - 9% work from an office
 - 7% work from a coworking space
 - 5% work from a cafe
 - 1% work from elsewhere



Teleworking: The New Normal For Years to Come

Teleworking reduces carbon emissions through:

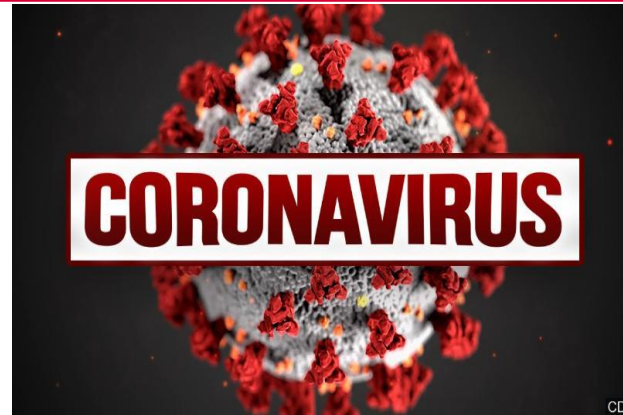
- Reduction in air travel
 - Reduction in office space
 - Reduction in commuting to work
- **Remote work:** A remote worker performs their work from a location other than their employer's physical office, such as from their home, a coworking space, or coffee shop.
 - **Telecommuting:** Employees work primarily outside of the office (often at home) but within commuting distance to their home office and occasionally attend meetings or conferences in the office.
 - **Virtual job:** This position provides 100% location independence. Companies with this position often have no physical offices.



zoom

BLANKROME

The Redesigned Office



- The trend of the open workspace may be ending for good, and instead:



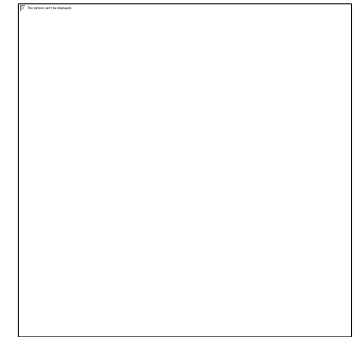
Home Office



Outdoor Office Space



Sanitizing UV Light



BLANKROME

COVID-19 Implications Beyond: Employer Demands

Employers Push:

- Use of secure conferencing software
- Use of Virtual Private Networks (VPNs)
- Regular (perhaps daily) software and security updates
- Training as employee susceptibility to hacks such as “phishing scams” continues to be the most vulnerable parts of employer networks
- Ensure employees have minimum connecting speeds
- Employers demand to protect confidential information and trade secrets not only from hackers but from those with access to employee laptops/home offices
- Employers will demand restrictive covenants more regularly and with stricter clauses



BLANKROME

COVID-19 Implications Beyond: Employees Pull: The *Pushback*

Employees Pushback:

- Employees need to protect personal information on their personal computers or networks
- Employees may pushback against an increasingly complex landscape of employer mandated requirements restricting competition, remote working locations, invasion of personal space
- Employees push back on being tracked



COVID-19 Implications Beyond: Discrimination & Inclusion

- Employers may find themselves involved in claims that they improperly used employee information that was accessible through the employee's personal computer or networks
- Anti-discrimination and harassment training is still required for a remote workforce
- Legal rules based on geographic considerations may change
- Employers should be cautious about how they choose who gets to work from home and that these decisions are not made in a discriminatory manner
- Hiring procedures based more on text or possibly exams with less of an emphasis on face-to-face interviews may decrease the opportunity for unconscious bias



COVID-19 Implications Beyond: Compensation

- Wage and hour issues will play a central role in the new remote work landscape
- Employers with employees working from home should ensure that employees are logging their time correctly
- Employers have shown concern regarding the amount of paid leave employees get and potential drops in productivity
- Employers may resort to relying more on contractors who are paid by the task instead of by the hour
- Cuts in cost-of-living differentials may be in order as employees can work where they live
- Payroll could prove more complex as employees spread out across multiple states



COVID-19 Implications Beyond: Health and Safety

- Workplace safety will also change considering the workplace is now the employee home
- Employers are still vulnerable to Workers' Compensation claims and should establish rules for their employees to ensure a safe workplace free of injury
- It is still unknown if the courts will interpret a COVID-19 infection occurring at a home office as a "workplace injury"
- Such demands on how workers set up their own homes may also produce employee pushback



BLANKROME

If you have questions, please contact:



Caroline Powell Donelan
Partner
Los Angeles
Labor & Employment
424.239.3476
cdonelan@blankrome.com



Stephanie Gantman Kaplan
Partner
Philadelphia
Labor & Employment
215.569.5381
sgkaplan@blankrome.com



Mara B. Levin
Partner
New York
Labor & Employment
212.885.5292
mlevin@blankrome.com

BLANKROME



Publications

article

6 Questions to Test Your Telework Compliance

Washington Technology

April 30, 2020

Government and contractors were unprepared for COVID-19 to so abruptly push so many employees to remote work. Even now, as businesses start to contemplate how to reopen their offices, the continued need for social distancing means many employees will be choosing or required to continue remote work for the foreseeable future. It's a fundamental change in how organizations operate, fraught with inconsistencies, challenges and distractions.

Yet, while the pandemic is causing modifications and deviations to contracts and regulations, it will not serve as a "Get Out of Jail FREE" card. Government contractors must still comply with their contracts and protect government information. What are the compliance implications of mass telework? Here are six questions to ask (and answer) to help you stay compliant while your employees are working.

To read the full article, please click [here](#).

"6 Questions to Test Your Telework Compliance," by Pat Fitzgerald* and Dominique Casimir was published on April 30, 2020, in [Washington Technology](#).

** Pat Fitzgerald is a director with Baker Tilly's government contractor advisory services group.*

Share This

PROFESSIONALS

Dominique L. Casimir

SERVICES

Government Contracts

Coronavirus ("COVID-19") Task Force

Labor & Employment

SPECIAL TOPICS

Coronavirus ("COVID-19") Task Force

6 questions to test your telework compliance

By Pat Fitzgerald, Dominique Casimir

Government and contractors were unprepared for COVID-19 to so abruptly push so many employees to remote work. Even now, as businesses start to contemplate how to reopen their offices, the continued need for social distancing means many employees will be choosing or required to continue remote work for the foreseeable future. It's a fundamental change in how organizations operate, fraught with inconsistencies, challenges and distractions.

Yet, while the pandemic is causing modifications and deviations to contracts and regulations, it will not serve as a "Get Out of Jail FREE" card. Government contractors must still comply with their contracts and protect government information.

What are the compliance implications of mass telework? Here are six questions to ask (and answer) to help you stay compliant while your employees are working remotely:

1. Are your telework policies and procedures up to date?

Resist the temptation to ignore telework policies that are suddenly impractical. In the absence of clear guidance, employees will be inconsistent in their behavior and performance. Take the guesswork out of the mix by updating and publishing revised policies. Provide clear, concise direction for what employees should do under current conditions (and new conditions, as government guidance evolves).

2. Is your IT infrastructure ready and secure?

A cyber-secure IT infrastructure built to support thousands of employees from a few offices will have vastly different loads and threats when most workers are suddenly piping in remotely. Is your VPN set up for the additional traffic? Do your security models and controls need to be adapted for the increased number of employees working remotely? Consider allowing access into the system for extended hours, so employees with family obligations have flexibility about when to do their work. Be sure your team fully appreciates the risks of relaxing some security controls (such as reducing keystroke monitoring) to improve your system's responsiveness.

3. Do employees have the technology and guidelines to work securely from home?

Most employees will do their best to serve government customers and be productive, even if they don't have the same technology at home as at work. But the bad guys in cyberspace are exploiting this crisis and are increasingly determined to test the security boundaries of governments, businesses and citizens. Some employee "best effort" behaviors could introduce unwanted compliance and security issues.

Remind employees of how to protect sensitive information at home. Re-publish policies about home network security, strong passwords, use of personal email accounts, unknown email attachments and other best practices. Consider home burn bags to store confidential papers until employees return to the office. Remind employees to disengage smart speakers in spaces where work-related conversations are happening. Use passwords and other added security measures for all video conferencing.

4. How are you managing and monitoring the productivity of remote workers?

Even veteran teleworkers have been disrupted by the sudden appearance of a spouse, children and/or roommates who are all competing for space, time, attention and internet bandwidth. Employees who are teleworking for the first time may have a home environment that is more casual, less vigilant, and filled with more distractions than an office setting.

It's important, though, to proactively manage and document the work employees are doing. Be sure employees understand policies about work hours, time tracking and status updates. Share tips and expectations for productive and professional telework. Task your managers to understand obstacles their employees are facing – and to communicate clearly about whether any temporary job accommodations are approved. Then, closely monitor performance to ensure that you're

delivering on your contracts and billing the government appropriately for the completed work.

5. Are key employees cross-trained?

Anticipate that key personnel may become unavailable to perform mission-critical duties at some point in the pandemic. If you haven't already, identify and cross-train employees who can step in should the need arise. Remember to obtain your customer's approval of these key employees, so work can continue uninterrupted. Keep an updated and centralized list or database to consult as your situation changes.

6. Are you monitoring your procedures and controls, especially the updated ones?

When so much is new and changing, monitoring your controls is a must to ensure timely corrective actions and prevent material non-compliances. Periodically test your company compliance hotlines to verify that they are accessible, appropriately staffed and supported. Keep your governance program (board of directors and executive committees) active, engaged, and available to address anything that might go awry.

COVID-19 has created a remote working scenario that most government contractors never could have envisioned. While it's different from anything we've experienced before, the government will not consider these changes an excuse for significant noncompliance. It is more challenging, but with planning, creativity and vigilance, companies, employees, and customers will be well served. In fact, you may find that some changes you make to accommodate the pandemic ultimately improve your operations and should endure after the crisis has resolved.

About the Authors

Pat Fitzgerald is a director with Baker Tilly's government contractor advisory services group, bringing more than 35 years of experience in government auditing and acquisition to every engagement. Pat supported the Section 809 Panel work and led the group that wrote the Professional Practice Guide. He previously served as the Director of the Defense Contract Audit Agency, and as the Auditor General for the U.S. Army.



Dominique Casimir is a partner in the government contracts practice of Blank Rome LLP. She assists federal contractors in responding to Civil Investigative Demands and government subpoenas, as well as conducting investigations and False Claims Act litigation. She also has extensive bid protest and claims litigation experience, as well as significant debarment experience. She is currently serving as co-chair of the ABA Section of Public Contract Law's Committee on Debarment and Suspension.





News and Views

media coverage

Bringing Select Workers Back Carries Litigation Risks: Experts

Business Insurance

May 12, 2020

Employers that are inviting select employees to return to work after COVID-19 shutdowns must tread carefully to avoid potential discrimination claims, experts say.

Without analysis beforehand, employers could leave themselves open to charges of violation of federal laws including the Americans with Disabilities Act, the Age Discrimination in Employment Act, and Title VII of the Civil Rights Act of 1964, as well as state and local laws.

[...]

If an employer returns a 35-year-old to a job but not a 65-year-old to the same position, based on a concern the older employee is more vulnerable to COVID-19, this could arguably be considered discrimination, **said Gus Sandstrom, a partner with Blank Rome LLP in Philadelphia, who defends and advises employers.**

"One thing we've been recommending when this comes up is, it's perfectly appropriate to reach out to employees in high-risk groups and inquire as to accommodations that may be possible," and whether they may prefer to stay home or return at a later date, Mr. Sandstrom said.

To read the full article, please click [here](#).

"Bringing Select Workers Back Carries Litigation Risks: Experts," by Judy Greenwald was published in [Business Insurance](#) on May 12, 2020.

Share This

PROFESSIONALS

Frederick G. Sandstrom

SERVICES

Labor & Employment

Labor Management Relations

Employment Litigation

Coronavirus ("COVID-19") Task Force

BUSINESS INSURANCE.

Bringing select workers back carries litigation risks: Experts

Posted On: May. 12, 2020 7:00 AM CST

Judy Greenwald

Employers that are inviting select employees to return to work after COVID-19 shutdowns must tread carefully to avoid potential discrimination claims, experts say.

Without analysis beforehand, employers could leave themselves open to charges of violation of federal laws including the Americans with Disabilities Act, the Age Discrimination in Employment Act, and Title VII of the Civil Rights Act of 1964, as well as state and local laws.

There is also the potential for wage and hour litigation, experts say.

They also point out that federal legislation now protects workers who cannot return to work because of child care issues.

Experts warn, too, that given the widespread unemployment created by the pandemic, some litigation may be inevitable, as desperate workers turn to it as a possible income source.

“This is a tough situation for business, because it is a unique thing. No one’s been through this before, and the guidelines are certainly changing, and it’s going to vary from state to state depending where you are in the country and what your local community is doing,” said Talene Carter, New York-based national employment practices liability product leader for FINEX North America at Willis Towers Watson PLC.

Decisions need to be made on an “unbiased, nondiscriminatory basis,” said Kelly Thorig, Richmond, Virginia-based U.S. employment practices liability product leader for Marsh LLC.

“The potential concern is not having a facially neutral criteria on bringing people back,” said Keith Gutstein, co-chair of the labor and employment practice at Kaufman Dolowich Voluck LLP in Woodbury, New York. “You can’t just pick your favorites and hope for the best.”

In deciding who will not return, employers should not target those who can be deemed susceptible to the coronavirus, such as older employees, pregnant women or individuals with pre-existing conditions, said Jason Habinsky, a partner with Haynes & Boone LLP in New York, who is chair of the firm’s labor and employment practices group. “Employers need to be prepared to accommodate rather than discriminate,” he said.

To avoid discrimination claims, employers should follow the same procedures they would in reductions-in-force by statistically analyzing whom they are asking to return and see if it is disparately impacting protected classes, said Tom Hams, Chicago-based managing director and national employment practices liability insurance practice leader at Aon PLC.

If that is the case, they must see if they “can justify the statistical anomaly. That’s the way to protect yourself,” Mr. Hams said.

Employers should be looking at skill sets, relative performance and evaluations, said Barry Hartstein, a shareholder with Littler Mendelson P.C. in Chicago, who is co-chair of its equal employment opportunity and diversity practice group.

“You may need individuals who are cross-trained and may be far more valuable,” Mr. Hartstein said. So it could be a question of “what are the skill sets we’re going to need in the new economy, because quite honestly we may be living in a new economy,” he said.

If an employer returns a 35-year-old to a job but not a 65-year-old to the same position, based on a concern the older employee is more vulnerable to COVID-19, this could arguably be considered discrimination, said Gus Sandstrom, a partner with Blank Rome LLP in Philadelphia, who defends and advises employers.

“One thing we’ve been recommending when this comes up is, it’s perfectly appropriate to reach out to employees in high-risk groups and inquire as to accommodations that may be possible,” and whether they may prefer to stay home or return at a later date, Mr. Sandstrom said.

There are also possible situations in which employees who are asked to return to work are too nervous to do so. “Employees are only entitled to refuse to work if they believe they are in imminent danger. This is a high bar to meet” under Occupational Health and Safety Administration regulations, said Melissa Camire, a partner with Fisher & Phillips LLP in New York, who represents employers.

“You should be taking steps to make the workplace a safe environment,” she said.

“That is a very slippery slope,” said Andrew Doherty, Valhalla, New York-based national directors and officers practice leader with USI Insurance Services LLC.



“There’s not a lot of precedent for this situation, and I think there’s going to be a lot of unique situations about what level of fear you have” with respect to the ADA “and what is a disability and what is a reasonable accommodation.”

Employers need to figure out what is a reasonable accommodation and what isn’t, Mr. Doherty said, adding, “Of course, there are situations where employers do have to move and get work done.”

Another possible source of claims is the federal Families First Coronavirus Response Act, which took effect April 1 and is set to expire Dec. 31. It requires employers to give employees paid emergency family and medical leave and emergency paid sick leave. The law covers private employers with fewer than 500 employees and certain public employers.

Experts warn an increase in litigation over the return-to-work issue may be inevitable. Currently, there are not many claims, because employees are collecting unemployment benefits that in some cases are more than what they would have made from their regular salary, Mr. Gutstein said.

But that situation may change, when companies start bringing people back and some workers are excluded, “when the unemployment runs out and there’s no other income,” or when they find their salaries have been cut, he said.

Employment practices liability policies “cover your traditional discrimination type claims,” including for retaliation and wrongful termination, “but EPL policies do have bodily injury exclusions, so it’s really going to depend on the specific wording of your EPL policy, and also how the claim is alleged, Ms. Carter said.

“If it’s straight discrimination and no bodily injury allegations, chances are it will trigger the policy, but with this pandemic it’s really hard to say how some of the claims will be alleged,” she said.

Wage and hour litigation is also possible, experts say. With more people working from home “you have much less control over tracking hours worked” and meal and rest breaks, Ms. Carter said. “I think we’re going to see more claims in terms of failure to pay overtime.” There may also be claims regarding the time it takes to wait in line to have temperatures taken when entering the workplace.

More insurance and risk management news on the coronavirus crisis [here](#).

COVID-19 Return-to-Work Checklist



PLANNING TO REOPEN

- ☐ Determine when reopening is permitted by state and local law and when it is best for your company
- ☐ Develop timeline for reopening and consider possibility of phased return to work
- ☐ Coordinate with landlord or management company regarding specific building protocols
- ☐ Develop contingency plans in case offices must close due to COVID-19 exposure
- ☐ Identify essential and non-essential employees for in-office operations
- ☐ Determine when and whether to recall furloughed employees and develop recall plan
- ☐ Consider union/CBA obligations regarding return-to-work preference, scheduling, and other issues; engage union leadership where appropriate

RETURNING EMPLOYEES TO THE WORKPLACE

- ☐ Develop communication plan to notify employees of plans to reopen and company expectations
- ☐ Consider whether to encourage continued remote work by certain employees and develop/update policies to handle remote work requests
- ☐ Develop transportation plans to encourage safe commuting—parking subsidies, company-hired vans/busses, education on safe commute practices
- ☐ Consider implementing staggered schedules for employees—different arrival/departure times or rotating in-office and remote work schedules

WORKPLACE SAFETY

- ☐ Review CDC and OSHA standards and state/local public health orders to determine specific workplace safety requirements
- ☐ Develop employee health screening protocols—temperature checks, health questionnaires, and/or virus and antibody testing
- ☐ Develop cleaning protocols for shared/common areas, employee workstations, and offices
- ☐ Develop policies to promote employee hygiene—hand-washing breaks, increased availability of sanitizer and cleaning supplies
- ☐ Educate employees regarding best practices for hygiene—no handshakes, hand-washing frequency, face coverings, cough etiquette
- ☐ Where possible, implement social distancing by rearranging workstations, controlling access and spacing in common areas (reception, conference rooms, kitchens, restrooms), restricting or eliminating in-person meetings
- ☐ If employees use shared workspaces, consider minimizing shared equipment by providing disposable desk covers, individual computer equipment, etc.
- ☐ Consider marking one-way path of travel in hallways and other common areas
- ☐ Consider whether to require or recommend that employees wear masks, face coverings, gloves, or other protective attire (PPE where required)
- ☐ Develop policies for third-party access to premises—vendors, couriers, package deliveries, guests

- ☐ Develop policies regarding employee travel and potential isolation requirements following return from travel
- ☐ Designate employee points of contact for safety concerns—both company-wide and on each floor or in each work area
- ☐ Develop policies and processes for COVID-19 workplace safety complaints

LEAVE AND ACCOMMODATION POLICES

- ☐ Review and update employee leave policies to address FFCRA/state law requirements and to consider unique circumstances (childcare, etc.)
- ☐ Review updated DOL, EEOC, and state/local guidance regarding employee accommodation obligations specific to COVID-19 pandemic
- ☐ Consider flexibility and specific policies for COVID-19 leave or accommodation requests, including due to personal and family health concerns
- ☐ Clearly communicate policies and expectations to employees

OTHER CONSIDERATIONS

- ☐ Communicate regularly with employees regarding safety practices, responses to employee concerns, and updates on COVID-19 workplace matters
- ☐ Consider adjustments to hiring policies—require virus or antibody testing as a condition of job offer

RECOMMENDED POLICIES AND DOCUMENTS

- ☐ Workplace reopening communications—reopening letter, furlough recall letter, remote employee return letter
- ☐ Office hours and scheduling policies—telework, rotational work, staggered scheduling
- ☐ Updated employee leave policies—FFCRA and state COVID-19 leave, if applicable, and other adjustments to existing leave policies, with associated employee communications
- ☐ Safe workplace policy—temperature checks / health screening, COVID-19 testing [optional], social distancing, employee hygiene, third-party access, mail/delivery requirements, office cleaning and sanitizing, use of common spaces, PPE requirements, and other COVID-19 safety matters

- ☐ Internal checklist for safety modifications (examples: elevator policies, one-way hallways, common area seating, relocating workspaces/cubicles, hand sanitizer stations, six-foot distance markings, touchless modifications, restroom modifications)
- ☐ Procedures for confirmed/suspected workplace exposure to COVID-19
- ☐ Procedures for COVID-19 accommodation requests
- ☐ Procedures for raising and handling COVID-19 complaints (safety, accommodations, etc.)
- ☐ COVID-19 updates to hiring policies and new hire communications
- ☐ COVID-19 updates to existing EEO, Anti-discrimination, Retaliation, ADA, and OSHA policies.

For additional information, please contact:

Brooke T. Iley, Co-Chair, Washington, D.C.
202.772.5816 | iley@blankrome.com

Jason E. Reisman, Co-Chair, Philadelphia
215.569.5598 | jreisman@blankrome.com

Susan L. Bickley, Partner, Houston
713.228.6620 | sbickley@blankrome.com

Stephanie Gantman Kaplan, Partner, Philadelphia
215.569.5381 | sgkaplan@blankrome.com

Anthony A. Mingione, Partner, New York
212.885.5246 | amingione@blankrome.com

Frederick “Gus” Sandstrom, Partner, Philadelphia
215.569.5679 | sandstrom@blankrome.com

Natalie Alameddine, Associate, Los Angeles
424.239.3454 | nalameddine@blankrome.com



Publications

article

How Businesses Can Fight Surging Email Compromise Scams

Law360

May 2, 2020

As the novel coronavirus continues to spread across the globe, cyberattacks seeking to exploit the crisis are similarly on the rise.

The frequency of COVID-19 business email compromise schemes — a particularly low-tech, but highly damaging type of cyber scam — has risen significantly in recent weeks, so much so that it prompted the Federal Bureau of Investigation to issue two alerts warning businesses of the growing threat.

As such, businesses must take appropriate measures to effectively mitigate the enhanced risk posed by BEC fraud, which is expected to increase even further in the coming weeks and months.

BEC Scams Explained

BEC scams, also known as CEO fraud and "man-in-the-email scams," involve tricking victims — often those who perform legitimate funds transfers — to make unauthorized wire transfers or send funds directly to the coffers of cybercriminals.

The typical BEC scheme originates with the theft of a corporate executive's credentials by phishing or other means. With those credentials in hand, cybercriminals will then impersonate the executive, sending urgent messages to lower level employees with requests to transfer or wire funds to bank accounts.

According to the FBI's internet crime report[1], the bureau received approximately 24,000 complaints concerning BEC fraud last year, with losses totaling \$1.7 billion — accounting for nearly half of all cybercrime-related losses in 2019. While ransomware frequently garners headlines due to the operational disruption caused by these attacks, cybercriminals have had much more financial success with BEC scams, netting at least 17 times more per incident (\$75,000) than ransomware (\$4,400).

It should come as a no surprise, then, that BEC was far and away the top source of cyber-related financial loss in 2019. BEC fraud is a relatively low-tech and low-cost scam that provides criminals with the ability to focus on high-value targets and high returns, all with minimal risk. This confluence of factors makes BEC scams particularly popular with cybercriminals.

Recent Proliferation of BEC Scams Tied to COVID-19

Over the years, cybercriminals have become more advanced and sophisticated in their attack techniques and methods, leading them to consider the psychological aspect of their scams.

Fraudsters have become extremely adept at exploiting current events — such as terrorist attacks and natural disasters — and the impact on the targets of their scams. As the COVID-19 crisis has deepened over the course of the last month, cybercriminals have adjusted their BEC scams to place a greater emphasis on COVID-19 and enhance the social engineering aspect of their attacks.

For example, BEC fraudsters are impersonating vendors and requesting payment outside the normal course of business, citing reasons relating to COVID-19 for the request. Similarly, cybercriminals claiming to be company executives are emailing lower-level employees requesting urgent, confidential wire transfers to cover costs due to unexpected issues arising from COVID-19.

FBI Issues Back-to-Back Alerts Warning of Anticipated Rise in COVID-19 BEC Schemes

Recently, the FBI issued back-to-back alerts warning of the enhanced threat of COVID-19 BEC schemes.

In its first alert,[2], the FBI warns that cybercriminals are actively exploiting the uncertainty surrounding the COVID-19 pandemic to further the effectiveness of their BEC scams. In particular, the FBI reports that it recently observed a significant spike in BEC fraud targeting organizations purchasing personal protective equipment or other supplies needed in the fight against COVID-19.

The FBI further cautions businesses to anticipate an even greater rise in BEC schemes tied to the COVID-19 pandemic moving forward.

In its second alert,[3] the FBI advises that cybercriminals are targeting organizations that use popular cloud-based email services — i.e., hosted subscription services that enable users to conduct business via tools such as email, shared calendars, online file storage and instant messaging — with an increasing number of BEC scams.

The FBI notes that in doing so, cybercriminals are using tailored phishing kits designed to mimic and impersonate cloud-based email services, making these scams extremely hard to detect as fraudulent.

Moreover, the FBI also reports a troubling trend of cyber criminals accessing the address books of compromised accounts to identify new targets and send phishing emails, allowing a single successful email account compromise at one business to be pivoted to multiple victims within an industry.

Analysis and Risk Mitigation Tips

BEC fraud has continued to grow, evolve and become significantly more sophisticated and deceptive in recent years. As such, BEC scams now represent one of the most destructive types of security threats faced by companies across all industries.

And like many other types of security threats, the prevalence of BEC scams has risen precipitously in recent weeks as the COVID-19 pandemic progresses, with fraudsters aiming to exploit the expanding scope of the crisis.

Moving forward, these same groups will continue to target businesses and individuals with new BEC schemes for the foreseeable future — such as with messaging targeting government stimulus payments set to be disbursed in the coming weeks. Even after the COVID-19 crisis has been put behind us, this type of attack will likely continue to increase, both in frequency and in the extent of losses experienced by victims.

Taken together, those entities that fail to take action to fortify their cyberdefenses against BEC attacks do so at extreme peril. Fortunately, there are several actionable steps businesses can take to mitigate the enhanced risk of BEC scams, including the following:

Cyber and Data Security Policies and Procedures

Businesses should have the proper policies and procedures in place to effectively mitigate the risk of BEC scams and other types of cyberattacks. Often, BEC scams involve the use of deceptive emails designed to appear as though they have originated from a superior or coworker.

Consequently, it is especially important to maintain a detailed corporate communications policy setting forth specific guidelines as to how the company will communicate securely with other members of the organization, which is vital to preventing employees from being tricked into complying with requests from malicious third parties.

Employee Education and Training

Businesses should adequately educate and train their employees on the issue of BEC attacks. Workers should be made aware of the significant threat posed by BEC fraud and the devastating consequences that would result if the company fell victim to an attack of this nature. Businesses should also educate employees on the most common BEC scam scenarios and how to respond in the face of any attempted attacks.

At the same time, businesses should provide workers with tips and best practices to follow to avoid falling victim to these scams, including: (1) exercising vigilance when responding to any last-minute changes in wiring instructions/recipient account information; (2) being cautious of high-level executives making unusual requests and requests from others expressing an abnormal sense of urgency; and (3) checking hyperlinks for misspellings of legitimate domain names or wrong domains (such as an address that should end in ".gov," but which ends in ".com" instead).

Cultivate a Security-First Workforce and Work Culture

Businesses and management should regularly communicate information, tips and tools regarding cyberattacks and cybersecurity generally to all members of their workforce. As vigilance is essential to thwarting BEC attacks, businesses must consistently instill in employees the importance of remaining alert of the ongoing threat of BEC scams — especially during this period when COVID-19 will continue to dominate headlines for the foreseeable future.

Organizations can quickly develop a culture and mindset that maximizes employees' commitment to making cybersecurity a top priority in their day-to-day activities, which in turn can play a significant role in stopping BEC scams and other types of cyberintrusions before they have a chance to wreak havoc on a company's operations and finances.

Utilize Effective Technical Defenses

Organizational defenses against BEC scams often rely exclusively on employees being able to spot attempted attacks as they occur. However, businesses that widen their defenses to encompass more technical measures as an added layer of security can significantly improve their chances of avoiding attempted BEC attacks.

Businesses should implement multifactor password authentication, which prevents cybercriminals from leveraging compromised employee email accounts if their credentials are obtained through phishing attacks or other cybercampaigns.

Maintain an Up-to-Date Incident Response Plan

Finally, businesses should anticipate that a percentage of BEC attacks will prove successful, as planning for these incidents in advance will help minimize any damage caused. Businesses should maintain incident response plans that can be implemented immediately and with adequate resources to respond to an executed BEC scam.

These plans should also be reviewed by key personnel to ensure they are up-to-speed on their roles and responsibilities in the event the plan needs to be put into action.

Conclusion

Businesses must remain vigilant and take proactive steps in defending against the burgeoning security threat posed by BEC scams. At the same time, as cyberthreats continue to develop and evolve at a rapid pace, businesses must also stay current on the latest trends to stay ahead of the curve and effectively defend against these risks, which will remain active and substantial for the duration of the current public health crisis.

To fully manage and mitigate the enhanced risk of BEC scams, businesses should speak with experienced legal counsel to ensure they have the proper policies, procedures and protocols in place to combat these potentially lethal attacks to the greatest extent possible.

And if a business suffers a successful BEC attack or other type of security incident during the COVID-19 crisis (or any time thereafter), experienced counsel should be contacted as soon as possible to provide immediate assistance with rapid response and crisis management, which is key to minimizing the fallout and impact of a breach event.

“How Businesses Can Fight Surging Email Compromise Scams,” by Jeffrey N. Rosenthal and David J. Oberly was published in [Law360](#) on May 1, 2020.

[1] FBI, 2019 Internet Crime Report, https://pdf.ic3.gov/2019_IC3Report.pdf.

[2] FBI, FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic, (April 6, 2020), www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.

[3] FBI, Cyber Criminals Conduct Business Email Compromise Through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than \$2 Billion, (April 6, 2020), www.ic3.gov/media/2020/200406.aspx.

Share This

PROFESSIONALS

Jeffrey N. Rosenthal

David J. Oberly

SERVICES

White Collar Defense & Investigations

Coronavirus (“COVID-19”) Task Force

INDUSTRIES

Artificial Intelligence Technology
Cybersecurity & Data Privacy
Data Privacy

SPECIAL TOPICS

Coronavirus (“COVID-19”) Task Force

AUTHORS

Jeffrey N. Rosenthal
David J. Oberly

FIND AN ATTORNEY

A B C D E F G H I J K L M N O P
Q R S T U V W X Y Z

OFFICES

Chicago, IL
Cincinnati, OH
Fort Lauderdale, FL
Houston, TX
Los Angeles, CA
New York, NY
Philadelphia, PA
Pittsburgh, PA
Princeton, NJ
San Francisco, CA
Shanghai
Tampa, FL
Washington, D.C.
Wilmington, DE

SUBSCRIBE

Register to receive insights and analyses on breaking news and trends across varying industries.

LOGIN

REGISTER

Enter details to create an account

First name

Last name

Email address

JOIN NOW

VISIT PARTNER SITE

ROME

CONNECT

Twitter

LinkedIn

Blogs



© 2020, Blank Rome LLP. All Rights Reserved. Attorney Advertising. Disclaimer. Privacy Statement. Privacy Notice for California Residents.

CORONAVIRUS

MARCH 2020 • NO. 2

How to Approach Coronavirus-Related Workplace Scenarios

COVID-19 (commonly referred to as the “coronavirus”), a respiratory illness that was first diagnosed in Wuhan, China, in late 2019, has hit the United States. The World Health Organization (“WHO”) has declared the outbreak a public health emergency of international concern and the virus is being classified as an epidemic. With the spread of the virus, employers face a series of constantly evolving questions regarding their competing legal obligations to provide a safe workplace.

While the immediate risk of contracting COVID-19 in most workplaces remains low, many federal agencies, including the U.S. Centers for Disease Control and Prevention (“CDC”), have issued [specific guidance](#) for employers to respond to the disease. This client alert discusses recommended approaches and alternatives to specific situations affecting employees in the workplace. Implementation of these recommendations may need to be tailored to your particular business, with consideration being given to workplaces with employees who work in concentrated spaces; employees who have greater exposure on a daily basis with the public; employers who can easily transition to remote working arrangements; and employers who can afford to pay healthy employees to stay home.

WHAT SHOULD AN EMPLOYER DO IF AN EMPLOYEE...

...is sheltering a self-quarantined person?

The CDC does not recommend testing, symptom monitoring, or special management for people exposed to asymptomatic people with potential exposures to the virus. These people are not considered to be exposed and therefore are categorized as having “no identifiable risk.” As a result, there are no extraordinary precautions that need be taken other than those imposed on all employees, which is to stay home if they are feeling sick. Of course, employers can take extra precautions that they deem necessary.

...is exposed to a symptomatic person?

If the employee has no elevated risk of exposure, such as an underlying medical condition or is over 50, that person is considered to have no identifiable risk. As long as that person remains asymptomatic, the CDC does not recommend testing or restriction on movement, but simply continued self-observation for any symptoms.

...is exposed to a confirmed case but is asymptomatic?

This will vary from no identifiable risk to low risk to medium risk depending on the exposure.

Brief exposure: If an employee is briefly exposed to a confirmed case—meaning they did not come in close contact (within six feet) nor were they in proximity to the person in the same indoor environment, the CDC considers this to be no identifiable risk.

Exposure in the same indoor environment, but not close contact:

If the employee was exposed to a confirmed case and was in the same indoor environment but not in close contact, they are considered low risk. Recommendation for low risk is to ask the employee to work remotely, if possible, and, if not possible, that employee should be asked to self-monitor.

Self-monitoring means people should monitor themselves for fever by taking their temperature twice a day and remain alert for cough or difficulty breathing. If they feel feverish or develop measured fever, cough, or difficulty breathing during the self-monitoring period, they should self-isolate, limit contact with others, and seek advice by telephone from a healthcare provider or their local health department to determine whether medical evaluation is needed.

Close contact with a confirmed case: If the employee was exposed to a confirmed case and was in close contact, like a household member, that person is considered medium risk. The CDC recommends those at medium risk remain at home—but not in close contact with the person who was diagnosed—and conduct active monitoring.

Active monitoring means that the state or local public health authority assumes responsibility for establishing regular communication with potentially exposed people to assess for the presence of fever, cough, or difficulty breathing.

...is symptomatic?

Employee should remain at home for 14 days from the time of exposure and engage in active monitoring.

...is diagnosed?

Offices are closing where someone in the working environment was diagnosed with COVID-19 despite the CDC stating that those employees who did not come into close contact with the infected employee remain at low risk. However, since it is often difficult in many workplaces to know who actually came into close contact with an infected employee, in an abundance of caution, companies are sending everyone home.

...refuses to work because of fear of contracting the virus?

Under the Occupational Safety and Health Administration (“OSHA”), the employer has a legal obligation to provide a safe and healthful workplace for employees. However, an employee is only entitled to refuse to work if they believe they are in imminent danger, which is defined as a danger that can reasonably be expected to cause death or serious physical harm. Assuming this employee is not in a high-risk category, they do not have the right to refuse to come to work without that imminent danger being present.

Of course, an employer should consider the reaction from their workforce in requiring employees to come to work even with an unfounded fear of infection, and devise a policy that makes sense for both their business and the welfare of their valued employees.

...wants to wear a face mask at work?

Since the CDC does not recommend that people who are well wear a face mask to protect themselves, face masks should only be worn by those who are showing

symptoms to protect others. Therefore, employers are within their rights to advise employees that they cannot wear a face mask while in the office. Face masks provide a false sense of security to the employee looking to be protected and alarms others who believe the employee wearing a face mask is sick.

However, as with all the recommended guidelines, employers need to consider their particular working environment and workforce. If employees want to wear a face mask despite the false sense of security, and it is clearly communicated that those doing so are seeking to protect themselves, and not because they are sick, then, employers may want to allow their employees to do so (especially in an office environment where they are not interacting with the public). In that event, an employer should issue a written policy that lets the employees know they are permitted to wear a face mask to protect themselves and reinforces that if they are sick they need to stay home.

Blank Rome continues to advise on these and other emerging issues, draft communication and business continuity plans, and create and adapt disease prevention policies for employers of all sizes operating in the United States and globally. Please contact a member of the [Labor & Employment](#) group with any questions—no question is too small.

For additional information, please contact:

Mara B. Levin, New York Office
Partner, Labor & Employment
212.885.5292 | mlevin@blankrome.com

Brooke T. Iley, Washington, D.C., Office
Co-Chair, Labor & Employment
202.772.5816 | iley@blankrome.com

Taylor C. Morosco, Los Angeles Office
Associate, Labor & Employment
424.239.3826 | tmorosco@blankrome.com



News and Views

media coverage

Seven Worst Compliance Fails of the Coronavirus Pandemic

Compliance Week

May 5, 2020

Some companies dealing with shutdowns, disruptions, sickness, and shortages rose to the occasion. But many have stumbled, misjudged the risks, did not have a business continuity plan, or fumbled its implementation. Here are seven of the worst compliance and ethics fails of the coronavirus pandemic—so far—with (hopefully) some lessons learned:

[...]

3. Coronavirus infections have plagued essential workplaces

Beyond PPE shortages, another glaring problem “has been very poor communication between employers and their employees,” **said Gus Sandstrom, partner with the employment law firm Blank Rome**. Employers should explain their current situation with PPE as clearly and often as possible, he said. That includes informing employees when PPE will be available and what steps they can take in the meantime to protect themselves.

“Employees want to know their company is trying to take care of them,” Sandstrom said. “In most situations, employees are willing to give employers the benefit of the doubt.”

Even employers struggling to obtain enough PPE can show they care for employees by doing everything possible to reduce transmission by cleaning workspaces; spacing employees at least six feet apart; staggering work start and stop times to reduce crowding; taking temperatures of employees before work, sending anyone home who shows symptoms of coronavirus; and notifying affected employees if one of their co-workers falls ill, Sandstrom said.

“Seven Worst Compliance Fails of the Coronavirus Pandemic,” by Aaron Nicodemus, was published in [Compliance Week](#) on May 5, 2020.

Share This

PROFESSIONALS

Frederick G. Sandstrom

SERVICES

Coronavirus (“COVID-19”) Task Force
Labor & Employment

Quarterly Review

Volume 14

Issue No. 1

Spring 2020

OHIO ASSOCIATION *of* CIVIL TRIAL ATTORNEYS

**A Quarterly Review of
Emerging Trends
in Ohio Case Law
and Legislative
Activity...**

Contents

President's Note	1
<i>Jamey T. Pregon, Esq.</i>	
Introduction:	2
<i>Ian D. Mitchell, Esq.</i> <i>Professional Liability Committee Chair</i>	
New Paycheck Protection Program Offers Forgivable Loans To Small Businesses	3
<i>Rema A. Ina, Esq.</i>	
Balancing COVID-19 Concerns and the ADA in the Workplace	5
<i>Rafael McLaughlin, Esq. and Leslie Kizziar, Esq.</i>	
Absolute Means Absolute: Understanding and Applying The Attorney Litigation Privilege	7
<i>Kurt D. Anderson, Esq.</i>	
Compliance Tips for Law Firms and Lawyers To Minimize Cyber-Related Legal Liability	18
<i>David J. Oberly, Esq.</i>	
Avoiding Heightened Cyber Risks During COVID-19	21
<i>Getchen K. Mote, Esq.</i>	

Compliance Tips for Law Firms and Lawyers To Minimize Cyber-Related Legal Liability

David J. Oberly, Esq.
Blank Rome LLP



While no type of business is immune to hackers today, law firms in particular have found themselves to be especially vulnerable and susceptible to criminal cyber activity, with firms of all sizes experiencing more attempted—and many times successful—cyber attacks from malicious

outsiders and data compromise events stemming from firm employees. At the same time, the scope of potential legal liability exposure faced by law firms in connection with data compromise events has also expanded rapidly as well. As such, firms must take proactive measures to shield client data from unauthorized access and acquisition, which can be accomplished through the implementation of several key data security measures as part of an overall cyber risk management program. Executed properly, effective law firm cybersecurity measures can protect law firms not only from experiencing a catastrophic data breach incident, but from substantial potential liability exposure as well.

The Noteworthy Cyber and Security Threat Faced by Law Firms

Cyber attacks on law firms have become so commonplace today that it is no longer a matter of *whether* a firm will fall victim to a cyber-attack, but a question of *when* and *to what extent* a cyber-attack will occur. There are several reasons why law firms are such magnets for cyber attacks.

First, law firms possess a treasure trove of sensitive client data—data which has significant value—rendering them a principal target of cyber attacks aimed at accessing that private firm data, which is then sold on the black market. Second, law firms have money, and lots of it, making them the ideal target for ransomware attacks, where cyber

criminals can make easy money by locking down a firm's files until a ransom payment is made.

Third, law firms today are still generally ill-prepared to deal with the sophisticated cyber attacks that are being carried out by cyber criminals today. Broadly speaking, the operation of law firms is still not managed as closely or efficiently as other businesses. Despite the growing threat, many firms have failed to take note and implement the appropriate policies, procedures, and other safeguards that are required to mount an effective defense against today's sophisticated cyber attacks. For the malicious hacker, then, a law firm's computer network may be much easier to penetrate than that of its client.

Increased Scope of Cyber-Related Legal Liability Faced by Law Firms

To further complicate matters, law firms face significantly expanded potential cyber-related legal liability as compared to years past.

First, the threat of legal malpractice claims stemming from data breach incidents or other cybersecurity-related failures is no longer merely theoretical, but now constitutes an actual and significant threat to law firms. While relatively few malpractice claims have been pursued by clients against their attorneys to date, the increasing standards that are rapidly developing regarding the implementation of proper data security safeguards will inevitably lead to an increase in the number of cyber-related legal malpractice claims that are filed as time progresses.

In fact, that trend has already started, first in *Shore v. Johnson & Bell*, No. 16-cv-4363 (N.D. Ill. 2016), a class action lawsuit that was filed against a Chicago law firm for alleged cyber vulnerabilities and failing to protect the security and confidentiality of its thousands of clients

and former clients. Similarly, in *Millard v. Doran*, No. 153262/2016 (Sup. Ct. N.Y. Co. 2016), a legal malpractice action was filed against a New York attorney for allegedly lax data security measures that allowed cyber criminals to send fraudulent instructions to a client during a real estate transaction which, in turn, caused the client to erroneously wire \$2 million in funds to the account of the hacker.

While both of these cases were resolved shortly after suit was filed and without an adjudication on the merits, *Shore* and *Millard* provide plaintiffs with a clear blueprint for pursuing legal malpractice claims against law firms and attorneys in the wake of a data security incident involving clients' sensitive or confidential personal information.

Furthermore, in addition to targeted legal malpractice claims, law firms and attorneys are also now vulnerable now to more general negligence claims arising from inadequate cybersecurity measures and data breach incidents. For example, in *Dittman v. UPMC*, 196 A.3d 1036 (Pa. 2018), the Pennsylvania Supreme Court held that employers have an affirmative duty to take reasonable care to safeguard sensitive personal information possessed by the company from cyberattacks. The *Dittman* ruling is a watershed event in cybersecurity and data breach litigation, as the decision establishes new rules of the road for negligence claims asserted in the wake of data breach incident. Importantly, the *Dittman* ruling is applicable well beyond only the employer-employee relationship, and likely applies with equal force in other contexts, including attorney-client relationships.

In addition, law firms and lawyers now also face liability in connection with new consumer privacy laws that are starting to be enacted across the country. For example, the California Consumer Privacy Act of 2018 ("CCPA")—which went into effect at the start of 2020—requires companies, including law firms, to comply with a range of requirements and limitations regarding the collection, use, and sharing of personal data of California residents. In addition, the CCPA provides consumers—including law firm clients—a private right of action to pursue class action litigation in connection with certain data breach events, with available statutory damages of \$100 to \$750 per incident. Other state legislatures across the nation have made a concerted effort to enact similar "CCPA copycat" laws of their own, and it is highly likely that other states will be successful

in putting in place their own versions of the CCPA in the coming months and years.

Compliance Steps

Combined, law firms and lawyers face noteworthy potential legal liability in connection with data breaches and other types of data compromise events. Fortunately, there are several proactive measures that firms and attorneys can take to minimize the risk of cyber-related legal liability:

- **Cybersecurity/Data Security Policies & Procedures:** As a starting point, firms should develop and implement a stringent set of cybersecurity and data privacy policies and procedures addressing the use of technology by firm personnel. These policies should define expectations for employees, as well as anyone with access to firm data, regarding issues such as the use of personal email and devices, file-sharing programs, the copying of data to personal devices, and use of firm systems from remote locations. Important policies to have to reduce the risk of cyber-related legal liability include acceptable use, Internet use, mobile device and tablet, bring-your-own device ("BYOD"), and password policies.
- **Firm Personnel Education & Training:** Education and training is a second vital ingredient to any effective firm cybersecurity risk management program, as many data compromise incidents are either directly or indirectly caused by human error or carelessness. In particular, firm employees should be made aware of the vital importance of safeguarding firm data and the key role that firm personnel play in ensuring the security of the organization's networks and systems. Furthermore, firms should also educate personnel on effective cybersecurity practices, such as being suspicious of potential phishing emails, and the ability to spot social engineering schemes, which have become a go-to tactic for hackers attempting to infiltrate firm networks through human vulnerabilities.
- **Maintaining a Security-First Firm Culture:** Beyond mere education and training, firms should also strive to promote a cybersecurity-first culture throughout their organizations. This can be done in a variety of ways. Set achievable, firm-wide security goals. Connect the security of the firm to the personal privacy of employees

CONTINUED

themselves. Communicate clear rules and requirements regarding the use of technology at work. Educate employees about the business benefits, and potential severe negative consequences, that employees' cyber habits have on the firm. Post reminders around the office relating to cyber-attack prevention measures. Combined, with the proper amount of time and effort, firms can develop a mindset and culture throughout the organization that maximizes employees' commitment to making cybersecurity a top priority in their day-to-day activities, which in turn can play a significant role in preventing cyber attacks from wreaking havoc on a firm's systems and finances.

- **Vendor Management:** In addition to assessing the security of their own systems, firms also need to assess the security of their vendors as well, as law firms' support vendors can often serve as the weakest link in a firm's security chain due to inadequate security controls and the entry portal these entities possess to firm systems. As part of the vendor selection process, firms should conduct thorough due diligence and evaluate the vendor's data security practices and procedures. Once a vendor is retained, firms should ensure that vendor access to firm data, as well as the vendor's ability to make changes on the firm's system, is limited to the greatest extent possible. In addition, firms should also develop necessary contractual security requirements for all vendors that maintain access to the firm's client information or systems.
- **Cyber Insurance:** Finally, firms should obtain cyber-specific insurance coverage (if they have not already done so) to mitigate the risk of expenses and losses resulting from a data breach incident. Law firms cannot assume that their general firm insurance policies will cover all losses stemming from a cyber attack, as many firms have discovered the hard way that their professional errors and omissions insurance, general liability insurance, and property insurance do not cover all of the costs associated with a cyber attack. Cyber insurance coverage, on the other hand, is specifically designed to cover losses stemming from a data breach, both in terms of response costs for things like providing notice of a breach, as well as damages and expenses arising out of lawsuits stemming from the breach. Importantly, in addition to covering direct

losses stemming from a breach, cyber-risk policies will also cover indirect costs and expenses associated with the breach, such as public relations firm costs, legal fees, and credit monitoring services fees.

Conclusion

Due to the massive volume of sensitive, highly valuable client information that is collected and maintained, as well as the noteworthy amount of revenue generated, law firms are particularly prime targets for cyber attacks. Recently, malicious hackers have stepped up the frequency and sophistication of their attacks against law firms large and small, with firms now facing far greater security threats than ever before. Cyber attacks on law firms are only likely to escalate and intensify moving forward, as cyber criminals develop new techniques to infiltrate firm systems and networks in more advanced ways. At the same time, firms and attorneys also face significantly expanded liability in connection with cybersecurity and data security incidents as well.

As such, it is critical for law firms to implement effective measures to properly safeguard their networks and systems, as well as the data they possess. Through the implementation of the cybersecurity practices and safeguards discussed above—as part of a comprehensive cybersecurity risk management program—law firms can take proactive precautionary measures to effectively minimize the risk of falling victim to a cyber attack and, more importantly, avoid being on the receiving end of a potentially catastrophic cyber-related lawsuit arising from cybersecurity and data security shortcomings.

David J. Oberly, Esq. is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Cybersecurity & Data Privacy and Privacy Class Action Defense groups. David's practice encompasses both counseling and advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters, as well as representing clients in the defense of privacy and biometric privacy class action litigation. He can be reached at doberly@blankrome.com. You can also follow David on Twitter at @DavidJOberly.