

Checklist

A General Counsel's Guide to Preparing for Coronavirus Investigations

*Adam S. Hoffinger, Douglas I. Koff, Barry A. Bohrer,
and Noah N. Gillespie, Schulte Roth & Zabel*

Reproduced with permission. Published May 2020. Copyright © 2020 The Bureau of National Affairs, Inc.
800.372.1033. For further use, please visit: <http://bna.com/copyright-permission-request/>



A General Counsel's Guide to Preparing for Coronavirus Investigations

Contributed by *Adam S. Hoffinger, Douglas I. Koff, Barry A. Bohrer, and Noah N. Gillespie, Schulte Roth & Zabel*

Businesses of all sizes are grappling with a variety of issues related to the coronavirus crisis: the employment, cybersecurity, and privacy concerns stemming from remote workforces; whether to apply for federal funds to resume operations when communities reopen; and how to adapt to such profound change and significant uncertainty about the future.

The federal government will increase enforcement initiatives during and in the wake of this crisis, as has historically occurred after times of market dislocation. General counsel at companies large and small cannot afford to wait until things are “back to normal” to position themselves to withstand increased government scrutiny. Company counsel can take the following steps now to prepare for investigations following the coronavirus pandemic.

Shaping Adaptable Policies and Procedures

Your business likely looks much different now than it did even two months ago. The instinct to just follow the company's standard policies and procedures is understandable. However, even though significant changes can be costly because they require reeducating the workforce and increase the risk that past practice will not match the new policy, you may need to make changes to protect your business.

The government often views harshly companies that do not follow—or in the government's view, live up to—their standard policies. But, given the change in circumstances, the government may conclude that any company that failed to adapt its policies to meet the new realities of the coronavirus crisis behaved inappropriately. The best approach is to apply the same careful thinking and regular testing you would normally employ, on a faster timeline, while documenting in detail the reasoning and knowledge that motivated making any changes or maintaining the status quo.

- Convene a team that is as lean as possible while reflecting the entire breadth and depth of your business, so that it can take into account differences among departments and the changing environment.
- Canvass on a global level all of the policies and procedures of the firm, aiming to keep most of the standard policies in place while identifying the areas that will need to change to properly foster compliance in the current environment.
- Revise and reissue the vulnerable policies and procedures in a way that keeps them adaptable and ready to be tested soon after their implementation. “Lean startups” get to market quickly by trying something out with the ability to nimbly adjust their offerings incrementally, allowing customers to inform the startup what will sell best. Preserving flexibility is key in a crisis. Once you realize that a policy needs to change, introduce the solution as a working policy that will evolve, then test and seek feedback to identify the policy that will achieve the optimum effect in the real world.
- Adjust the normal procedure for testing the effectiveness of policies to be more frequent, to help you detect pressure points and aspects that may not be working.
- You are likely operating based on a business continuity plan (BCP) that has never been tested on this level before. Collect the lessons already learned and adjust the BCP so it can carry your business through the duration of this crisis.
- Regulations that require recordkeeping still apply even though your workforce is now at home and doing much more of their work from their personal devices and the company has embraced new video meeting software. For example, they may be making calls from cell phones rather than using an office line. While companies subject to recordkeeping rules have to emphasize to their employees the importance of preserving all the required records, all companies have to keep in mind the new risks inherent in the use of personal devices, from increased cybersecurity threats to privacy issues.

- If a subsequent government investigation reveals that communications were lost because they were made on personal devices or on applications not supported by the firm, or because the firm's regular document retention procedures caused them to be destroyed, unfavorable consequences may ensue. Consider revising document retention procedures to collect and retain all business communications from the start of the crisis.
- Enforce policies that ensure the firm can access information related to the business while respecting employees' privacy. In this regard, consider reminding employees that they have no reasonable expectation of privacy in firm-provided technology and systems.
- Prepare a framework for the return to normal. Identify which aspects of the BCP will sunset first and which should remain longer. Plan how will you make clear which policy governs what conduct at each point in time.
- Consider creating more channels for employees to raise concerns quickly, so leadership learns of potential issues before they cause problems. And create proper infrastructure to receive and process this increased body of information. Consider identifying who will receive the information and training that group to identify what issues need to be raised to upper management.
- Make sure to document in detail the decisions discussed above and the reasoning for them.

Investigating Internally to Identify Problems

As you test the effectiveness of your policies you will find lapses, which left undetected and uncorrected could lead to government scrutiny and investigation. You should make the most now of the lessons to be learned from any problems you encounter as your best protection against any enforcement action later.

- The mistake you find may not be the only one. Learn from errors you detected to identify any similar issues and to identify ways to find new issues you had not anticipated.
- Take action that communicates to everyone that compliance is an essential activity that is still happening during the crisis.
- Get to the bottom of the conduct. As this fact-finding can be intensive, outside counsel may be best positioned to find the facts while keeping leadership free to focus on the business. Involving outside counsel can also give the strongest attorney-client privilege and attorney work product protection to the investigation.
- Remediate the problem. Identify steps that will minimize the likelihood that the error will happen again and that will enable you to demonstrate to the government you have corrected the issue.
- Consider reporting requirements. For example, many states require reporting the occurrence of a data breach to authorities within a set period of time. Beyond just complying with the legal requirements, however, consider in consultation with outside counsel whether, when, and how to report your findings to the government at your own initiative, rather than waiting for the government to call.

Training From Afar

Communication with and training employees will be crucial as the business of maintaining corporate compliance shifts. After all, policies and procedures mean little if they do not permeate actual practice. With many workforces going remote and sharp reductions in travel, the way companies perform training has to change.

- Communicate with employees on a regular basis. More frequent contact will provide opportunities to share new developments as they happen.
- Conduct training in a manner in which employees can readily participate. Video seminars may not work for every business or every department. In some circumstances, small group chain trainings may better accomplish the goal, with each team leader delivering the message to their direct reports, all using a single company-generated guide.

- Borrow a page from the cybersecurity playbook: One best practice following a training session on phishing emails is to send a fake phishing email to employees where the suspicious link directs the employee to a page with further phishing training. Consider ways to reinforce the subject of the training soon after employees attend. While only some scenarios are amenable to this falling-into-the-safety-net approach, other scenarios can be reinforced with follow-up messages in different formats, so employees have adequate opportunities to absorb the key takeaways.

Avoid Becoming a Victim

Working to keep employees and agents on course with the business's compliance demands is only part of the picture. Fraud and opportunistic behavior will no doubt be prevalent in this crisis, and certain businesses are most at risk.

- Every business faces increased cybersecurity risk. With more users connecting to the network, employees working remotely, and less in-person authentication of requests, many of the practices that helped protect the business before are not good enough now.
- Many Ponzi and pyramid schemes get exposed during financial turmoil because losses become so great that the perpetrator of the fraud cannot hide them. Given recent market losses, businesses should redouble their diligence on existing and potential new investments.
- Companies should be on the lookout for counterfeit goods. As more states require employers to provide personal protective equipment for essential employees, the demand on these items will only increase, and with it the risk that you will buy a counterfeit product that may itself pose a danger to your staff.
- Any company that receives funding from the government, or applies for funding during the crisis, must be careful to make truthful and accurate statements in seeking and maintaining that funding. Misrepresentations in obtaining government funds during the crisis is not just a reputational hazard for your business, but will be an obvious focus for government enforcement during and after the crisis.
- Industries that are heavily impacted by the crisis itself, including tourism, hotels, airlines, retail, and health care, are ready victims for scams. The more desperate the state of the business becomes, the less vigilant officers and employees will be to threats.

Keep Investors Informed

Public companies are obligated to keep the investing public well informed. They must disclose material developments, and ensure that the public receives that information simultaneously with or before discussions about that development with smaller groups. Companies that are not publicly traded may have fiduciary duties to observe. Because companies must correct prior communications that may have become inaccurate, reviewing and updating disclosures is a necessary ongoing activity. Securities and Exchange Commission Chairman Jay Clayton and the Director of the Division of Corporate Finance William Hinman recently [emphasized](#) the importance of corporate disclosure and indicated the attention SEC staff will likely direct to the disclosures companies are making right now. Consider:

- How have the nature and goals of your business changed as a result of the crisis?
- To what extent are your future plans limited to the duration of the crisis, such that it would be inappropriate to yet predict the plans you will undertake as the crisis eases?
- Are there deals, projects, or initiatives you previously announced that are now delayed, shelved, or abandoned, and have you updated investors on these developments?
- What will your ongoing success depend upon?
- What risks does the business face that it did not face before? Have any prior risks been removed or eclipsed?

If you happen to determine there is any concern about being insolvent or seeking bankruptcy protection, what timeline do you have under applicable law to first make those decisions, and thereafter report them to investors? Although general counsel are ordinarily well-equipped to deal with most challenges in-house, the current environment puts a premium on efficiency. With so much changing so rapidly, a focus on keeping the business going may result in losing sight of the big picture. Outside counsel can refocus that picture and take on worthwhile investigations with minimal disruption on officers' time and attention.

It is clear the government is not waiting for the crisis to end to take action. Companies must take care now to best position themselves to avoid—and if necessary weather—a later legal crisis.