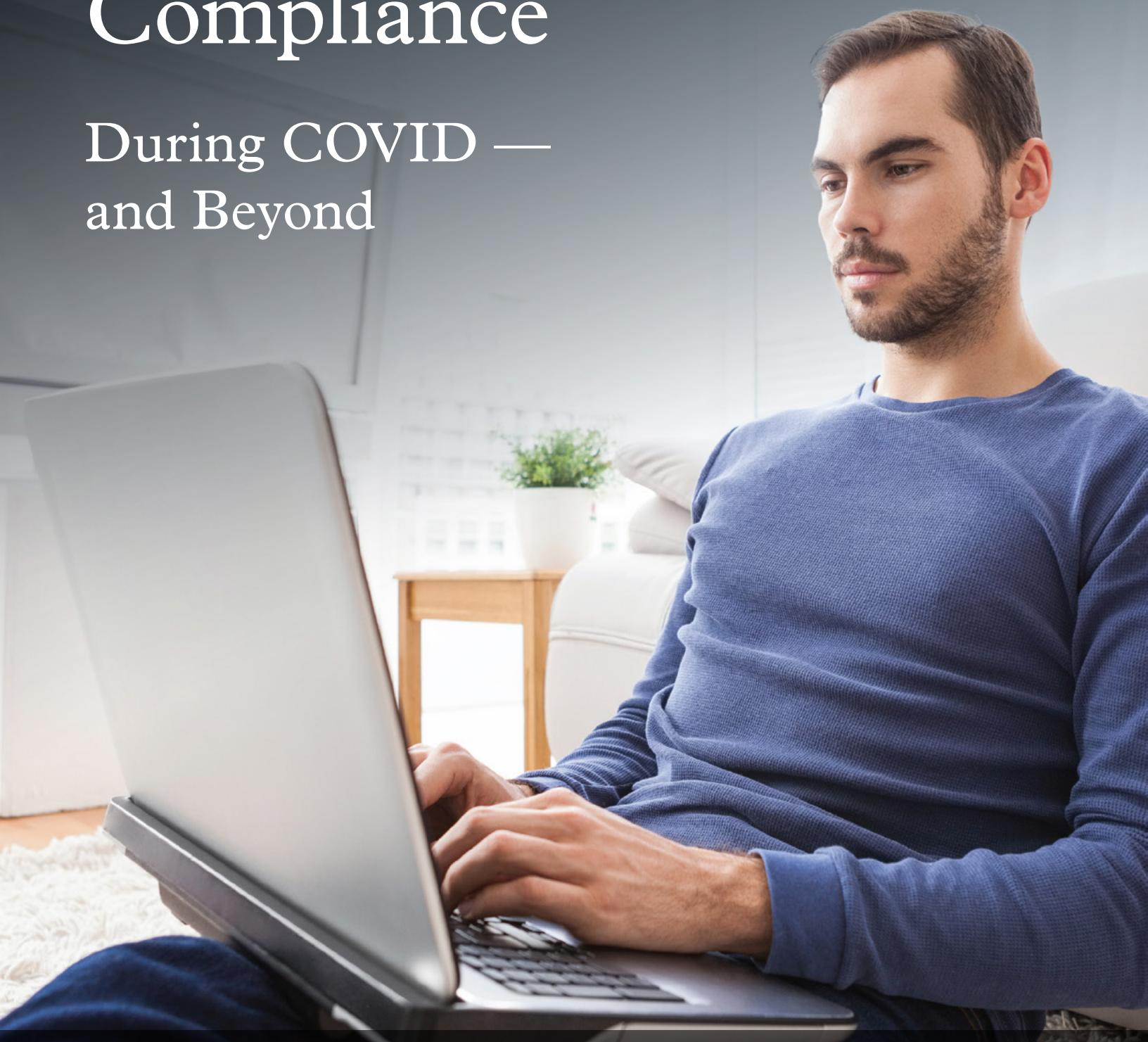
Steele Compliance Wave

Interactive Whitepaper

Communicating Compliance

During COVID — and Beyond



info@compliancewave.com 241 Maple Avenue, Suite 201, Red Bank, NJ 07701

EXECUTIVE SUMMARY

In March 2020, millions of workers abruptly shifted from business-as-usual to indefinite remote work — almost overnight.

And with this fast pivot to remote work, thousands of companies opened themselves up to new compliance challenges:

- Communication failures
- Relaxed standards
- Cyberattacks
- Fraud proliferation
- Third-party disruption
- COVID spread

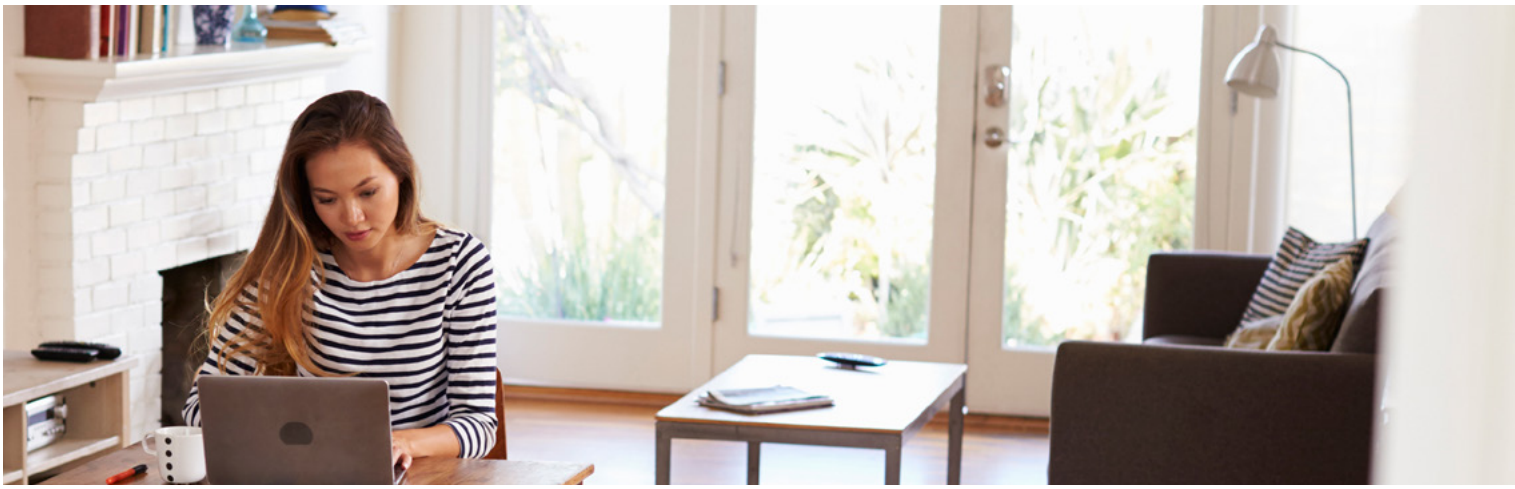
In this comprehensive guide, we'll look at the emerging compliance risks businesses face in 2020 and the most effective strategies for tackling them.

Let's dive in.

Interactive Whitepaper:

This whitepaper has clickable links to examples and samples that tend to the content in each section. Click to explore them.

Click where you see this graphic



THE NEW COMPLIANCE LANDSCAPE

Managing compliance risks within your organization is always a challenge. And our new remote reality has made it more challenging than ever.

In 2020, many companies made a fast pivot to remote work for the first time. Between February and May 2020, 35.2% of U.S. workers switched from office-based work to working from home. By the end of May, about half of all U.S. workers were working remotely.[1]

These changes will have long-lasting effects on the American workforce. While approximately 13% of U.S. workers were remote prior to the pandemic, experts project that 23% of the workforce will continue to work remotely after COVID-19, as physical distancing measures and the increasing ease of remote work makes it a more widely accepted option.[2]

Even under normal circumstances, compliance management isn't easy. And with the rapidly evolving risks of our new remote reality, effective compliance management is more challenging than ever.

Let's take a closer look at the changes compliance professionals are facing in 2020.

Companies like Facebook, Twitter, and Shopify are leading the way...

...by offering permanent work-from-home arrangements to many employees.

Experts estimate that up to **56% of the workforce** hold jobs that could potentially transition to fully remote in the years to come.[3]

How Compliance Risks Are Shifting

With the pivot to remote, transitions that would normally have been planned over many months or even years happened on the fly, often in less than a week.

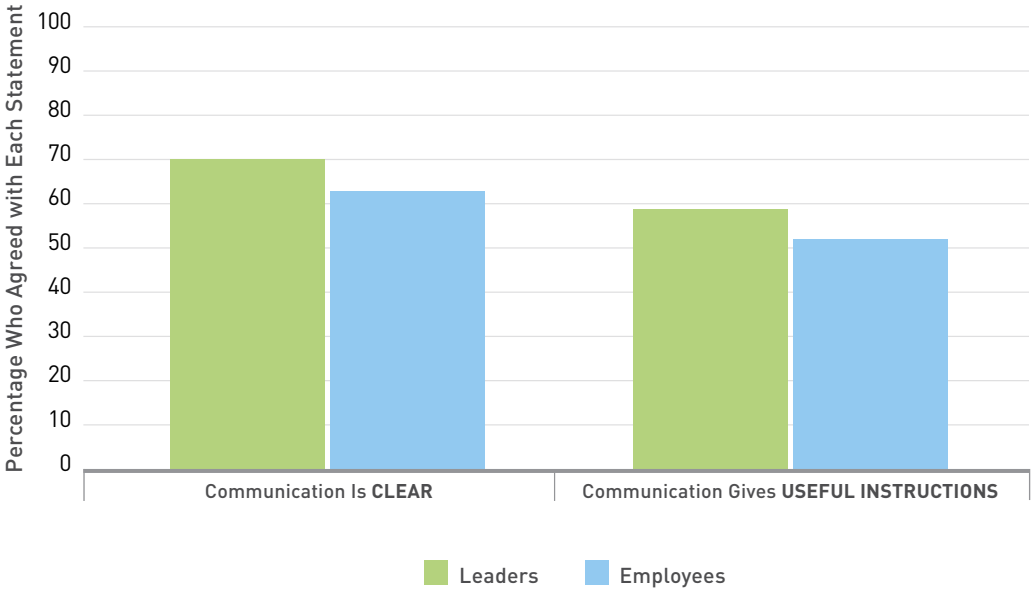
In this totally unexpected situation, organizational leaders were often improvising solutions as they went along. And that created new challenges for professionals charged with compliance and risk management. Here are a few ways the pandemic has changed the game for compliance professionals.

Communication Breakdowns

81% of communications executives surveyed in March 2020 stated that consistent communication with employees was a high priority for their COVID response. But just 41% said that their organization's communication function was very prepared to respond to COVID.[4]

Organizational leaders and employees agree that communications are often lacking in areas relevant to managing compliance risks. In a survey on the effectiveness of organizational communication during COVID, over 30% of both groups agreed that their organization's communication was not clear — and over 40% stated that messaging was not useful.[5]

Organizational Communication During COVID



Relaxed Standards

Perhaps the biggest challenge facing compliance professionals is a perception problem. With regulators signaling that they'll give firms increased latitude to improvise during the crisis, anyone in your organization might conclude it's acceptable to push normal ethical boundaries.

But as history shows, that's just not true. Think back to the 2008 economic crash. In the wake of the crash, many corporations were forced to pay unprecedented monetary penalties for failure to meet standard regulatory guidelines.

For example, after the 2008 crash, Bank of America paid a number of compliance fines, including $11 billion paid as part of a larger settlement with the nation's largest mortgage servicers in 2012. In 2014, they paid a $9.3 billion settlement with the Federal Housing Finance Agency. And that same year, Credit Suisse paid $2.6 billion in fines for helping thousands of taxpayers hide their assets in offshore accounts.[7]

IT Systems Under Attack

To accommodate large numbers of newly remote workers, many companies made incredibly fast changes to their IT infrastructure in early 2020. These changes opened a wide range of new compliance risks, including migration of data to personal devices, fast-tracked adoption of new software platforms, and careless handling of sensitive data.

Cybersecurity experts warn that these shifts have placed enterprise IT infrastructure at a greater risk of cyberattack than ever before. 94% say that the risk of cyber threat to enterprise systems and data has risen with COVID. Even more worrying, 70% expect to have to respond to a major security breach in their organization within the coming year.[8]

Experts point to three primary aspects of the remote transition that can cause increased risk.[9]

- Vulnerabilities in corporate remote access systems provided to remote workers
- Increasing phishing and social engineering attacks designed to take advantage of the crisis
- Vulnerabilities in the devices workers use to access enterprise data from home

Fraud Proliferation

The pivot to remote has impacted a wide range of business processes, opening new opportunities for fraud.

By mid-April, the FTC received over 18,000 reports of COVID-related fraud. And in a May 2020 survey, 68% of respondents to a survey of anti-fraud professionals reported witnessing an increase in fraud incidents — with 93% stating that they expected to see an increase within the next twelve months.[10]

Fraud prevention specialists highlighted these areas as most at risk of an increase:[11]

- 91% **Cyberfraud**
- 86% **Fraud by Vendors and Sellers**
- 85% **Payment Fraud**
- 84% **Health Care Fraud**
- 81% **Insurance Fraud**

Third Party Disruption

Of course, it's critical to look beyond your own organization for compliance risks. In a recent global survey of 170 organizations, 87% reported that they'd faced a disruptive incident with third-party partners in the last two years.[12]

Consider these risks:

- **Legal violations.** During a crisis, partners and suppliers are more likely to disregard legal and ethical regulations in order to weather the economic storm. Your organization can be held responsible for the conduct of third-party partners under the US Foreign Corrupt Practices Act (FCPA). Already in 2020, the Department of Justice and the SEC have pursued a number of actions against companies for FCPA violations.[13] In June and July 2020, respectively, the Department of Justice released an updated version of their guidance on Evaluation of Corporate Compliance Programs and the Second Edition of A Resource Guide to the U.S. Foreign Corrupt Practices Act, both of which reinforce the increased expectations of the DOJ.
- **Supply chain disruptions.** By February, 94% of Fortune 1000 companies had already reported supply chain disruptions to their operations. If your most critical vendors and suppliers don't have continuity measures in place, it can seriously impact your own business operations.
- **Data breaches.** Whenever organizations give third-partners access to their online data systems, they open themselves up to a potential security breach. And if your company isn't following best practices for conducting proper due diligence, you're particularly vulnerable to attempts by cyberattackers to access your data systems via third parties.

> "Protecting the health and safety of employees isn't just a legal responsibility. It's an ethical imperative."

COVID Spread

Most fundamental of all, companies must ensure the safety of their employees. In the United States, employees have the right to a safe workplace under the Occupational Health and Safety Act. Employers who fail to protect their employees' safety can face stiff penalties. By early April, OSHA had already received more than 3,000 complaints of unsafe work environments.[14]

Even if your company has transitioned to remote work, many of your team members may still be meeting in person with vendors or customers. It's essential to provide frequent communication to your team about steps they can take to stop the spread of the virus, whether they're at home or in the workplace.

Communication Strategies for Mitigating COVID-Era Risks

While the risks can be daunting, compliance teams can adapt to meet the emerging risks through ongoing communication and training. Let's take a closer look.

Preserving a Culture of Compliance

Preserving a strong compliance culture is an essential objective of a COVID-era compliance communication program. Compliance professionals can reduce the risks involved in shifting to a remote workforce by maintaining a strong compliance culture.

Creating and maintaining a strong compliance culture requires communication in three areas.

1. Communication from management emphasizing the company's commitment to INTEGRITY and an OPEN-DOOR POLICY
2. Risk-area specific communication and training that helps employees identify and respond to EVERYDAY COMPLIANCE ISSUES
3. Communication and training emphasizing that RAISING CONCERNS with the compliance office is encouraged

Communicating in all three of these areas is vital to maintaining a culture of compliance, especially during uncertain times. Unfortunately, COVID caused the cancellation of many live events and conferences. Compliance officers are no longer making in-person visits to reinforce the compliance message with managers or high-risk workgroups. The move to a remote workforce requires a shift from in-person communication to digital communication.

Communication must shift from long-form talks or training sessions to short, bite-sized bursts of information that employees can access whenever it fits into their day. Brief, focused communication is called microlearning. Read on to learn more about the key areas to focus on for success.

> "As we pivot to remote, microlearning is the perfect way to train employees on the key behaviors that will minimize risks across the organization."

“Upper management sets the tone for the rest of the organization.”

Upper Management

Key points that upper management must communicate include:

- We need to be even **more vigilant** in protecting our ethical reputation in these turbulent times.
- Every action must be completely **honest and fair**.
- **Ethical action** goes beyond compliance and the letter of the law.
- We encourage **dialogue** at all levels.
- We must all review and **adhere to the standards** contained in our Code of Conduct.

Middle managers face new communication challenges in the remote workplace that require a proactive response. Remind managers to:

- **Be alert to potential problem situations**, and genuinely encourage open discussion by welcoming questions and issues whenever they arise.
- **Allow people to speak up** when mistakes are made or if someone seems out of line. Create a workplace where everyone is respectful and also respects the company’s high performance standards.
- **Use staff meetings as a venue for discussion of ethical issues**, so employees see ethics as a normal consideration in any business decision.
- **Reports remain confidential** in the company’s investigative process, and results will not be revealed in public.
- **Act when an issue is raised.** Involve experts such as HR or the Ethics Office and take steps to initiate change.

In short, the job of management at all levels is to reinforce the company’s commitment to policies and principles contained in the company’s Code and to ensure that employees know where to turn when they have a concern.

See a sample communication tool here:
Leadership Message During COVID

See a sample training module here:
Compliance Brief Interactive: Code of Conduct Awareness

See a sample training module here:
Compliance Brief Interactive for Managers: Reporting Misconduct

Risk-Area Training and Communication

Several compliance areas present increased risks during times of turmoil or when employees are working remotely. On-going, topic-specific communication and training is essential to help employees navigate related compliance issues.

Maintaining IT Security

To help your employees stay vigilant about keeping the organization's data secure when working remotely, some best practices include:

- **Avoiding the use of any non-business** email address or other personal social media account for all business communications.
- **Encrypting** all emails and files sent to the cloud.
- **Using virtual private networking**, or VPN, rather than unsecured public WiFi.
- **Only downloading items from trusted sources.**

One significant threat to the security of IT systems and data comes from "phishing," that is, emails or other messages designed to get employees to download software that can contain viruses, collect usernames and passwords, destroy content or steal trade secrets. Phishing can be done by email, instant messaging, social media or phone.

Phishing is on the rise during COVID and employees need to be especially vigilant. In mid-April, Google's Threat Analysis Group reported that they were blocking approximately 18 million COVID-themed malware and phishing emails per day. And Microsoft reported a massive phishing campaign in May, in which emails that appear to be from Johns Hopkins prompt users to download files that install remote access tools on their computers. Phishing remains a critical topic, and training and follow up communication should occur frequently.

See a sample video here: **Working Remotely: Data Privacy and Information Security in a Crisis**.

Preventing Fraud

Combined with our uncertain economic conditions, the new remote reality creates an array of incentives and opportunities for employees to engage in fraudulent activity. Remind employees at all levels to be alert for the following:

- **Fast-tracked approval.** Disruptions in the supply chain and fast-tracked approval processes can open the door for employees to hire their own preferred suppliers even when there is a clear conflict of interest — or even create a completely fictitious vendor.
- **Incomplete documentation.** Under remote working conditions it can be challenging to verify management review and sign-off of documents — which can create an opportunity for employees to hide fraudulent activity.
- **Pressure to hit performance goals.** Particularly when organizational survival is at stake, employees might feel unusual pressure to meet performance goals in any way possible. These conditions can incentivize employees to commit fraud.
- **Competitive compensation schemes.** In organizations with competitive compensation schemes, workers fearful of losing their income or their job may feel the need to cheat the system.

See a sample training module here: **Compliance Brief: Fraud**

Working with Third Parties

The majority of our third parties share our values but, in the months ahead, you can expect some potential suppliers to cut corners to stay afloat. It's more important than ever for internal staff to conduct thorough due diligence and consider use of a negative news monitoring tool for higher risk third parties. Encourage them to ask lots of questions and carefully review all contracts and documents before they get started.

Here are some additional points to communicate to employees involved in managing third party relationships.

- It's more important than ever for **internal staff to conduct thorough due diligence** and consider use of a negative news monitoring tool for higher risk third parties.
- **Schedule regular monitoring** of existing suppliers for consistent performance with their contractual responsibilities.
- **Conduct regular on-site audits** of suppliers and their key suppliers with particular care for possible human rights violations such as child labor, trafficking, prison labor and unsafe working condition.
- **Pay close attention to third-party contracts** with consultants and advisors to ensure defined well defined duties and performance obligations and appropriate payment for such performance.
- **Ensure that contracts with third parties contain a right to audit their records.**
- **Consistently monitor financial records**, especially those related to billing, expenses, subcontractor fees, and any unusual costs.
- **Pay attention to anything that "doesn't look right."** It might not "be right."

Finally, **make clear your compliance expectations** to all third parties through training and communication.

See a sample training module here: **Compliance Brief: Anti-Bribery/AntiCorruption for Third Parties**

The Shifting Geography of the Pandemic

Pay special attention to the shifting geography of the pandemic. Suppliers based in areas that see a surge of cases can suddenly pose a high risk for supply chain disruption due to local shutdowns and stay-at-home orders — and many businesses are at a higher risk of failure due to the challenging economic climate.

To weather the storm, have a plan in place to turn to alternate suppliers to minimize disruptions to your operations.

COVID Spread

With Google recently announcing that their employees will stay remote through the summer of 2021, it's clear that COVID is expected to remain present in the US well beyond the end of 2020. Containing the virus requires continuous communication that highlights the risks and details the specific behaviors required, including:

- **Wear a mask** when in public.
- **Avoid large gatherings** of 10 or more people.
- **Wash your hands** frequently with soap and water, scrubbing for at least 20 seconds. Wash especially before handling food or eating.
- **Cough or sneeze into your elbow.**
- **If you develop symptoms, contact your doctor for advice.** Do not go immediately to the emergency room.

See a sample video here:
Preventing COVID-19

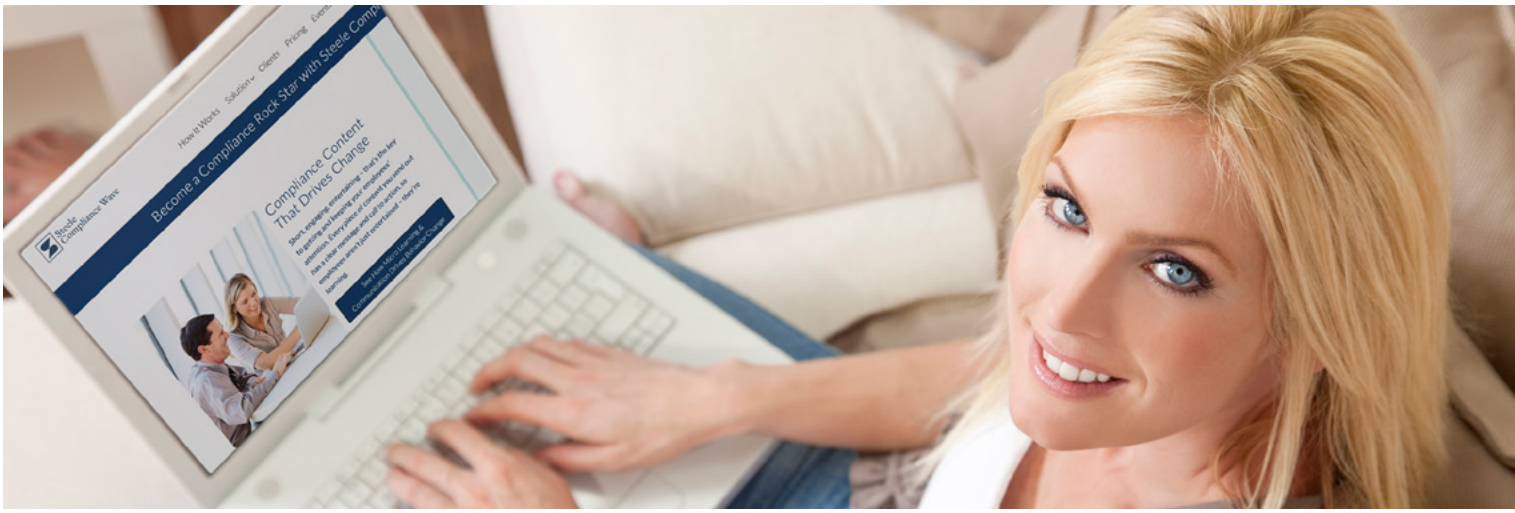
Reporting Misconduct

Misconduct increases during turbulent times. Even though the COVID situation is temporary, the impact of misconduct can have long lasting consequences. Remind employees that:

- Reports of observed or suspected wrongdoing are required of all employees.
- Many lines of communication are open for employees to use for responsible reporting, including upper management, Human Resources, the Ethics Office, and the Legal Dept.
- The Help Line provides an anonymous avenue for employee's reports.
- Reporting is essential for the health of our company. If you observe or are subjected to retaliation for your responsible reports, you must shed light on the situation so that it can be investigated and corrected.
- All reports are thoroughly investigated.
- False accusations are not responsible and can damage the morale of our company. You may be subject to discipline if you report in an irresponsible manner.
- The company has many resources, such as upper management, Human Resources, the Legal Department, the Ethics Office, and the Help Line in order to clarify your questions or to make a report.

See a sample training module here:
Compliance Brief Interactive: Reporting Misconduct 2nd Edition

"Although this is well-worn advice, the risk is that people become complacent as time passes, stop practicing these basic guidelines, and the virus reemerges."



Calibrating Your Communication for the COVID Era

COVID has transformed all our lives in unanticipated ways — and it's also transformed the work of compliance professionals.

Now that you know the new risks created by our remote reality, it's critical to respond with communication that helps people across your organization make the right choices.

As we've seen, you'll want to zero in on these areas of focus:

- **Maintaining IT security.** Ensure that employees understand best practices for keeping enterprise data safe and avoiding cyberattacks and phishing scams.
- **Preventing fraud.** Educate employees on emerging areas of risk for fraudulent activity to ensure that team members at all levels are keeping a watchful eye.
- **Working with third parties.** Take steps to reinforce the importance of due diligence with everyone involved in third party relationships, including regular monitoring of contractual responsibilities and on-site audits.
- **COVID spread.** Care for the health and safety of your team by communicating regularly on steps to take to prevent the spread of the virus.
- **Reporting misconduct.** Maintain a compliance culture with consistent messaging about ways to call out suspected wrongdoing.

References

1 Brynjolfsson, E., Horton, J., Ozimek, A., Rock, D., Sharma, G., TuYe, H. "COVID-19 and Remote Work: An Early Look at US Data." National Bureau of Economic Research. Retrieved June 28, 2020 from **https://www.nber.org/papers/w27344.pdf**. p. 1.

2 Institute for Public Relations. "Special Report: How Companies are Engaging Employees During COVID-19." Retrieved June 28, 2020 from **https://instituteforpr.org/wp-content/uploads/PC_IPR_Coronavirus_Phase2_FINAL-4-22_compressed.pdf**. p. 7.

3 Global Workforce Analytics. "Work-From-Home After COVID-19: Our Forecast." Retrieved June 28, 2020 from **https://globalworkplaceanalytics.com/work-at-home-after-COVID-19-our-forecast**.

4 Institute for Public Relations. "Special Report: How Companies are Engaging Employees During COVID-19." pp. 1, 3.

5 BusinessWire. "STUDY: Organizations Rising to the Challenge of COVID-19 Communications, but Needs Persist." Retrieved June 28, 2020 from **https://www.businesswire.com/news/home/20200403005278/en/STUDY-Organizations-Rising-Challenge-COVID-19-Communications-Persist**.

6 PlanetCompliance. "The Biggest Compliance Fines of the Decade." Retrieved July 27, 2020 from **https://www.planetcompliance.com/2019/12/28/the-biggest-compliance-fines-of-the-decade/**.

7 US Department of Justice. "Credit Suisse Sentenced for Conspiracy to Help U.S. Taxpayers Hide Offshore Accounts from Internal Revenue Service." Retrieved July 27, 2020 from **https://www.justice.gov/opa/pr/credit-suisse-sentenced-conspiracy-help-us-taxpayers-hide-offshore-accounts-internal-revenue**.

8 Wilson, T. "Black Hat Survey: Breach Concerns Hit Record Levels Due to COVID-19." DARKReading. Retrieved June 28, 2020 from **https://www.darkreading.com/threat-intelligence/black-hat-survey-breach-concerns-hit-record-levels-due-to-COVID-19/d/d-id/1338167**.

9 Wilson, T. "Black Hat Survey: Breach Concerns Hit Record Levels Due to COVID-19."

10 ACFE. "Fraud in the Wake of COVID-19: Benchmarking Report." Retrieved June 28, 2020 from **https://www.acfe.com/COVIDreport.aspx**.

11 ACFE. "Fraud in the Wake of COVID-19: Benchmarking Report." Retrieved June 28, 2020 from **https://www.acfe.com/COVIDreport.aspx**.

12 Deloitte. "Understanding Third-Party Risk." Retrieved June 28, 2020 from **https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-on-the-boards-agenda.pdf**.

13 Asner, M., Green, J., Nassikas, J., Bernstein, D., Carson, L. "Foreign Corrupt Practices Act Mid-Year Review." Arnold & Porter. Retrieved July 12, 2020 from **https://www.arnoldporter.com/en/perspectives/publications/2020/07/foreign-corrupt-practices-act-midyear-review**.

14 The Washington Post. "Thousands of OSHA complaints filed against companies for virus workplace safety concerns, records show." Retrieved July 27, 2020 from **https://www.washingtonpost.com/business/2020/04/16/osha-coronavirus-complaints**.

STEELE COMPLIANCE WAVE

Steele Compliance Wave, a Steele company, provides engaging compliance communication tools that utilize behavior-science principles to drive meaningful change. Leading global organizations use our global-leading compliance microlearning and communications libraries of content to reinforce understanding of compliance and ethics issues, foster commitment and solidify intentions among employees, agents and other third parties. The company is led by industry pioneers with more than 20 years of experience creating innovative communications and training solutions. Learn more about our approach, our team and effective compliance communication at **www.compliancewave.com**.

241 Maple Avenue
Suite 201
Red Bank, NJ
07701 USA

+1.732.704.9220
info@compliancewave.com
www.compliancewave.com