Compliance in a Time of Crisis

Skadden

April 30, 2020

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

Addressing the Evolving Risks

Warren Buffett said that "only when the tide goes out do you discover who's been swimming naked." Buffett was not talking about compliance programs in a time of crisis, but his wisdom applies there, too. The COVID-19 pandemic has companies facing unprecedented financial and operational challenges. Given these challenges, many companies may be forced to shift stretched resources and attention away from key business and operational units, including compliance. In doing so, however, past crises show the vital importance of maintaining an ethical culture and focusing resources and attention on heightened areas of risk because regulators will expect more — not less — from companies in crisis as they look to protect the market, consumers and businesses from fraud, price gouging and other forms of misconduct. This note examines specific areas of compliance concern that may arise from the COVID-19 crisis.

Trading/Market Manipulation/Competition

Significant increases in market volatility may lead to an increased risk of market abuse. The 2008 financial crisis, for example, sparked a wave of enforcement activity to combat irregularities and market failures. Today, as financial institutions and asset managers transition to remote working, surveillance over traders will become more difficult. Advances in technology allow remote supervision of employees, but it remains challenging to replicate the full suite of compliance measures normally available to businesses. Companies should consider implementing enhanced testing or sampling of transactions to demonstrate to enforcement agencies their commitment to compliance. They should likewise consider reinforcing the importance of compliance with antitrust and competition laws, as well as the risks posed by information sharing among participants in financial markets.

Anti-Corruption

Governments have become active procuring supplies required to combat COVID-19. Increased commercial interactions between governmental actors and commercial enterprises will increase the risk that corrupt payments are made to governmental officials in relation to government supported assistance programs, special licensing, and permitting and tender sales. All of these risks increase as companies face pressure to maintain business activity, revenues and earnings in the face of economic disruption. Government assistance programs are challenging to navigate and will present particular risks in emerging markets. In all jurisdictions, wait times for government-issued permits will increase, approval processes will become more complicated, and there may be opacity

with respect to regulatory requirements. Companies should be cognizant of potential corruption concerns surrounding interactions with government officials and new partners onboarded to address these evolving dynamics. In a recent statement, U.S. Foreign Corrupt Practices Act officials from the U.S. Securities and Exchange Commission (SEC) and Department of Justice recognized the impact of COVID-19 on compliance efforts, while requesting transparency and emphasizing their expectation that companies continue to detect and report misconduct, noting that "the rules very much apply."

Disclosure Issues and Accounting Fraud

During this period of economic turbulence, companies must ensure that disclosures to investors and clients continue to be accurate. In the wake of the 2008 financial crisis, failures to keep investors adequately informed of developing impairments to performance and assets resulted in numerous enforcement actions. While it may not be possible to predict the ultimate impact of COVID-19, public companies must consider disclosure obligations in real time as events unfold. On April 8, 2020, in a joint statement, SEC Chairman Jay Clayton and the SEC's Corporation Finance Division Director William Hinman emphasized the importance of disclosing current and forward-looking financial information to investors and market participants in light of the pandemic. The statement highlighted investors' particular interest in information concerning the impact of COVID-19, including how the company's operations and financial condition may change as collective efforts progress in the fight against COVID-19. The statement indicated that the SEC does not expect to second guess "good-faith attempts to provide investors with appropriately framed, forward-looking information." Recent SEC enforcement, however, has been focused on risk factor disclosure that is too generic or characterizes impacts as "possibilities" when they are actualities — highlighting the importance of the role of disclosure committees and robust internal communications as companies undertake careful assessments of risk factor disclosures surrounding COVID-19.

Cybersecurity

While WiFi security has steadily improved, home networks tend to be more vulnerable to cybersecurity breaches than company systems. Increased pressure to ensure that employees and systems are quickly up and running for remote work may result in inadvertently flouting important security measures. In all points of access, networks should have adequate protections, including firewalls and multi-factor authentication. Companies also should consider the necessity of system patching for virtual private networks (VPNs) and implementing enhanced system monitoring, in order to shore up vulnerabilities compounded by a remote workforce. Furthermore, companies should maintain vigilance against phishing and other social engineering cyberattacks. These techniques often focus on the creation of a false sense of urgency, and COVID-19 presents ample opportunity to exploit an anxious workforce. In addition to implementing prophylactic measures, companies should be cognizant of their ability to handle incident response remotely, as a failure to launch a timely and effective response may lead to greater damage from the cyber attackers and increased legal exposure, as data breach notification deadlines are not tolled by COVID-19.

Sanctions/AML

Sanctions enforcement has become a favored tool for governments pursuing geopolitical goals, with potentially significant penalties for violations. In recognition of COVID-19-related humanitarian trade needs and compliance challenges, recently published guidance by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) included a summary of existing exemptions and authorizations to provide humanitarian assistance under certain sanctions programs as well as a notice encouraging financial institutions and other businesses affected by the COVID-19 pandemic to contact OFAC if they anticipate delays in meeting regulatory deadlines. Notwithstanding the limited exceptions to certain sanctions regimes for humanitarian assistance, companies should not expect good intentions to be a defense to even technical violations, and compliance difficulties may warrant early communication with OFAC or other applicable regulators.

Financial institutions should remain vigilant with respect to both sanctions and anti-money laundering (AML) compliance despite comments by regulators — such as the Federal Reserve — acknowledging the uncertainty presented by the COVID-19 pandemic.

There has been no indication that compliance expectations have changed in response to the crisis, as U.S. and U.K. regulators continue to bring enforcement actions and issue regulatory guidance. For example, the U.S. Federal Financial Institutions Examination Council (FFIEC) announced on April 15, 2020, updates to its Bank Secrecy Act (BSA)/AML Examination Manual that emphasize the risk-based approach that institutions should take to BSA/AML compliance. Similarly, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) recently published an updated notice and FAQs to assist financial institutions in complying with their BSA obligations during the COVID-19 pandemic, and provided an online direct contact mechanism for financial institutions to communicate to FinCEN COVID-19-related concerns in the context of meeting their BSA obligations.

More generally, shifting supply chains may create new challenges (or opportunities) for businesses but also increases risks of transactions with sanctioned parties and strains existing screening and tracking tools. Where certain functions need to be prioritized over others, care should be taken to ensure that they are selected based on documented risk assessments.

Further Recommendations

Even amid the pressing concerns created by COVID-19, neglecting warning signs or failing to address improper behavior can have repercussions that last long after the immediate crisis has ended. Enforcement agency guidance on compliance remains applicable in times of crisis — there is no COVID-19 carveout — so companies must remain appropriately focused on core compliance challenges:

Ensure Continued Risk Assessments and Robust Internal Communications

Given the particular challenges of remote work in an uncertain environment, gatekeepers should consider creative strategies to address real time risks. Legal, compliance, audit and financial leaders could establish internal task forces or regular check-ins to address issues identified in hotline reports, audits and financial reporting reviews. Dashboard or similar summary reporting to C-suite executives and relevant board committees should be increased as much as is practical under the circumstances to maintain attention on compliance risks and solutions.

Prioritize Spend Around Key Risks

While it may be necessary to delay spend on certain issues, now more than ever management needs to identify and prioritize key compliance risks and direct resources on a risk-assessment basis. Indeed, in its April 20, 2020, notice, OFAC endorsed this view, noting that companies should adopt a risk-based approach when faced with "technical and resource challenges" created by the pandemic. If temporarily reallocating compliance resources to account for COVID-19 challenges is part of a risk-based approach, OFAC noted that it would "evaluate this as a factor" in determining its response to an apparent violation during this period. We expect other regulators may have similar expectations.

Where companies find it necessary to reallocate resources around compliance functions, it is critical that they document the risk analysis performed in connection with those decisions. Even where regulators may concede that such reallocations were necessary, they will want to "see the work" underlying the risk analysis.

Maintain Visible Compliance Presence

Compliance professionals and senior management should be proactive and visible during a time of crisis — even while working remotely — to actively set an appropriate tone from the top. Companies should consider focusing employees' attention on key areas of risk while reminding them that ethical and compliance obligations continue in times of crisis, whistleblower allegations will continue to be monitored and investigated, and compliance resources are available to assist where questions arise.

Compliance in a Time of Crisis
Contacts

Contacts

Bill Batchelor
Partner / Brussels
32.2.639.0312
bill.batchelor@skadden.com

Boris Bershteyn
Partner / New York
212.735.3834
boris.bershteyn@skadden.com

Jamie L. Boucher
Partner / Washington, D.C.
202.371.7369
jamie.boucher@skadden.com

Gary DiBianco
Partner / Washington, D.C.
202.371.7858
gary.dibianco@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Andrew M. Good
Partner / London
44.20.7519.7247
andrew.good@skadden.com

Ryan D. Junck
Partner / London
44.20.7519.7006
ryan.junck@skadden.com

Bradley A. Klein
Partner / Washington, D.C.
202.371.7320
bradley.klein@skadden.com

Steve Kwok
Partner / Hong Kong
852.3740.4788
steve.kwok@skadden.com

Colleen P. Mahoney
Partner / Washington, D.C.
202.371.7900
colleen.mahoney@skadden.com

Bernd R. Mayer
Partner / Munich
49.89.24449.5120
bernd.mayer@skadden.com

David Meister
Partner / New York
212.735.2100
david.meister@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Elizabeth Robertson
Partner / London
44.20.7519.7115
elizabeth.robertson@skadden.com

Khalil N. Maalouf
Counsel / Washington, D.C.
202.371.7711
khalil.maalouf@skadden.com

Rebecca M. Murday
Associate / London
44.207.519.7242
rebecca.murday@skadden.com