Four Securities Enforcement and White Collar Issues to Watch in a Post-Pandemic Environment

April 2020

With the COVID-19 pandemic causing unprecedented disruptions across America's social and economic life, many companies are rightly focused on the health of their employees and business continuity plans. As the situation stabilizes, however, we expect to see an uptick in federal enforcement and other regulatory activity. This is true for at least two related reasons. First, as with prior economic downturns, there may be significant political sentiment to target the perceived "winners" or "haves" as the situation stabilizes. Second, as with the 2008-2009 recession, the aftermath of the current situation is likely to expose conduct that appears questionable, particularly when viewed in hindsight by a prosecutor or a regulator. Below, we outline four areas to watch in the coming weeks and months in the U.S. Department of Justice ("DOJ") and U.S. Securities and Exchange Commission ("SEC") enforcement arena.

More Government Help Will Bring More Government Scrutiny.

Both federal and state governments have passed a variety of COVID-19-related aid bills. Most notably, at the federal level, the Coronavirus Aid, Relief, and Economic Security ("CARES") Act authorizes up to $2 trillion in government spending to combat the economic disruption caused by COVID-19, including loans and other economic relief. These programs have been discussed in detail in previous Baker Botts client alerts, which can be found here and here.

But carrots also bring sticks, at least potentially. The CARES Act creates a "Special Inspector General for Pandemic Recovery," ("SIG-PR") who is empowered to "conduct, supervise, and coordinate audits and investigations of the making, purchase, management, and sales of loans and guarantees, and other investments" made by the Secretary of the Treasury under the act.[i] The SIG-PR appears to be generally modeled on the Special Inspector General for the Troubled Asset Relief Program ("SIG-TARP"), which was created in the aftermath of the 2008 financial crisis.

Like SIG-TARP, SIG-PR does not have independent prosecutorial authority but has subpoena power and can refer investigations to entities that do, such as DOJ and SEC. SIG-TARP's website touts that "380 defendants" have been convicted of a crime or fined and that 24 enforcement actions have been filed as a result of the agency's investigations over the last 12 years. It is a fairly safe assumption that SIG-PR will seek to follow SIG-TARP's track record.

More generally, businesses obtaining government assistance should ensure any request for federal assistance is completely accurate and that they familiarize themselves with any restrictions on the use of government funds. A number of federal statutes, including the False Claims Act ("FCA"), provide criminal and civil penalties for intentional misstatements made to government authorities. We will likely see an increase in FCA and other investigations relating to alleged misstatements in applying for CARES Act or other government assistance or misusing government funds.

Increased Policing of Insider Trading and Other Disclosure-Related Regulations.

On March 23, 2020, the SEC's Co-Directors of Enforcement issued a somewhat unusual public statement, (i) noting that "corporate insiders are regularly learning new material nonpublic information ["MNPI"] that may hold an even greater value than under normal circumstances," and (ii) urging public companies to ensure they protect against the improper dissemination of MNPI, by being mindful of their selective disclosure policies and other regulations, including Regulation FD (or "Reg FD").

Concerning insider trading, there have already been public reports of investigations concerning trading by members of Congress after receiving potentially non-public information. To guard against insider trading, companies can take some practical steps to safeguard potentially material information. These include carefully considering who truly has a "need to know" the information before it is made public, and, if and when a decision is made to disseminate the information, ensuring that public dissemination is prompt and broad, including through a Form 8-K if deemed necessary. Further, regularly reminding employees and outside professionals of the importance of safeguarding non-public information is prudent, particularly in light of the SEC's announcement.

Relatedly, Reg FD generally prohibits the selective disclosure of MNPI. First enacted in 2000, SEC enforcement of Reg FD has been sporadic over the last 20 years. That said, last August, the SEC filed a settled Reg FD based enforcement action against a pharmaceutical company, alleging that the company improperly shared MNPI with sell-side analysts about a meeting with the Federal Drug Administration, before issuing a press-release or making any other market-wide disclosure about the meeting. Given that action, and the SEC's explicit reference to Reg FD in its March 24 announcement, we expect to see continued focus by the SEC on Reg FD issues in the coming months.

Increased Cases at the Intersection of Securities Enforcement and Cybersecurity.

Cybersecurity has been a focus for the SEC in recent years as well. In guidance published in February 2018, the Commission noted that "it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack . . . ." And since then, the Commission has brought a number of actions against companies for failing to disclose material cyber-breaches in a timely fashion.

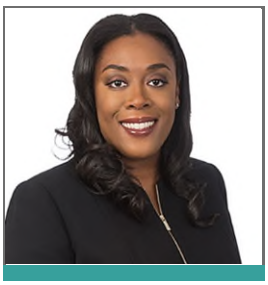
With much of the world's professional workforce working remotely, companies must be extra-vigilant about both encouraging employees to practice good cyber hygiene and ensuring their disclosures to investors about cybersecurity risks are accurate and up-to-date. Again, companies would do well to regularly remind employees, especially during this time, about using only company-approved electronic devices, not using personal email addresses for official business, and being extremely cautious about opening or responding to emails from unknown sources. A previous Baker Botts client alert, which can be found here, discusses some proactive measures companies can take to minimize the chances of a cybersecurity incident. Should a public company detect a cybersecurity breach, the company must consider whether that breach is material to investors. The SEC's February 2018 guidance notes that, in such situation, the Commission expects the company "appropriate disclose timely and sufficiently prior to the offer and sale of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk."

Impact on the Pace of Current Government Investigations.

While many investigations are continuing to proceed while DOJ and SEC employees work remotely, social distancing undoubtedly impacts the completion of many government investigations. For one, live testimony and in-person meetings, often seen by prosecutors as key to evaluating and "sussing out" witness credibility, are unlikely to occur in the current environment. Also, while some federal district courts have allowed grand juries to convene remotely, it is at least an open question whether individuals on a teleconference are truly "present" to make the required quorum of 16 grand jurors.

At the same time, the statutes of limitation generally require federal prosecutors to obtain an indictment within five years of the completion of an offense (six years for securities fraud). In civil actions, the SEC is also bound to a five-year statute of limitations. Legally, there are few avenues for prosecutors to seek an extension of the limitations period. As a result, we may see prosecutors and regulators (i) seek tolling agreements with increasing frequency, and/or (ii) look to rapidly conclude investigations as the pandemic subsides, which could lead to settlement offers with short turnaround times or rushed charging documents. Pre-charging discussions are often the best opportunity for a targeted company to minimize the risk of reputational harm and avoid misguided charges through strategic dialogue. However, this approach is most effective when the company has developed an evidence-based counternarrative, which requires time and access to witnesses. Targeted companies will need to carefully evaluate what progress can be made in the current environment and, if facing a rushed settlement or charging decision, whether to affirmatively raise the prospect of tolling the statute of limitations to preserve the opportunity for strategic dialogue.

Brendan F. Quigley
Partner
T: +1.212.408.2520
brendan.quigley@bakerbotts.com



Heather Souder Choi
Partner
T: +1.202.639.7859
heather.choi@bakerbotts.com

Kyle A. Clark
Partner
T: +1.202.639.1320
kyle.clark@bakerbotts.com

Joseph Perry
Special Counsel
T: +1.212.408.2587
joseph.perry@bakerbotts.com

[i] Under the Act, SIG-PR is required to report to Congress unreasonable refusals from government agencies to information requests. The President has taken the position that SIG-PR cannot make these reports without Presidential approval. Potentially, this sets the stage for conflict between the executive and legislative branches in which Congress seeks testimony or reports from SIG-PR, and the Executive Branch objects. However, we still expect the political winds will favor aggressive investigation of suspected fraud, waste, or abuse in connection with the $2 trillion aid package.