LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An ALM Publication

OCTOBER 2020

The Potential for Fraud or Misbehavior In the Time of COVID-19

By Julia Brickell

JB: There has been much attention focused on the likelihood of increased white collar investigations as we begin to emerge (albeit erratically) from the first wave of COVID-19. What have you been seeing so far? And what do you anticipate?

MB: The Coronavirus Aid, Relief, and Economic Security Act (the CARES Act) is a sweeping economic package of unprecedented size, which also has the potential for widespread fraud and abuse, and the inevitable investigation and prosecution of that conduct.

The CARES Act includes four principal accountability and oversight measures to address potential fraud and abuse: 1) the Pandemic Response Accountability Committee (PRAC); 2) a Special Inspector General for Pandemic Recovery (SIGPR); 3) increased funding for existing inspectors general; and 4) the Congressional Oversight Commission.

We expect that this environment of intense scrutiny will place significant pressure on PRAC, SIGPR, and existing oversight functions to investigate and identify bad actors and — together with federal law enforcement agencies, the Securities and Exchange Commission (SEC), and other civil enforcement agencies who may act on PRAC or SIGPR findings — to bring high-profile cases to punish and deter fraudulent or abusive conduct.

This will almost certainly include pressure to bring enforcement actions against corporate beneficiaries of the CARES Act, both because of a broad popular concern that large companies will benefit more than ordinary Americans, and because large companies are bigger targets, both financially and optically.

The new oversight functions also do not displace the government's existing enforcement tool kit, including garden-variety conspiracy and mail and wire fraud provisions, and the False Claims Act. This existing tool kit already is robust, and if anything, given the widespread political scrutiny of CARES Act programs, there may be pressure to apply the existing criminal and civil enforcement laws even more aggressively.

AM: On the advertising and marketing front the [Federal Trade Commission] FTC has been working around the clock to police and enforce against COVID-19 frauds of all sorts. These run the gamut from overhyped cure and prevention claims made by businesses and their owners or chief executives to consumers and scams targeting small businesses over deceptive stimulus payment claims. In many cases, the FTC is partnering with state attorneys general which have criminal authority that the FTC lacks. This will continue and the consumer protection enforcers will focus considerable enforcement resources to following the scams focused on consumers and small business owners. In addition, on the antitrust side the FTC, [Department of Justice] DOJ and the states are investigating and prosecuting price gouging of healthcare and PPE goods, sanitation supplies and, of course, toilet paper. Because these laws vary state to state, what is legal in one jurisdiction may be subject to criminal sanctions in another. This is a critical time for companies selling directly or who are involved in any way on the chain of distribution to look at their pricing policies closely.

Julia Brickell (JB), Executive Managing Director and General Counsel of H5, leads a roundtable on the topic of government investigations, corporate compliance efforts, and the potential for fraud or misbehavior in the time of COVID-19. The participants: **Gejaa Gobena (GG)** at **Hogan Lovells**, **Martine Beamon (MB)** at **Davis Polk**, and **Amy Mudge (AM)** at **Baker Hostetler**.

GG: On the front end, I have seen a lot of companies being cautious and thoughtful in how they are taking in federal aid, mindful of any potential False Claims Act or regulatory issues that may attach. With respect to enforcement, at least for DOJ-led criminal or civil fraud matters, I see it a bit differently. We haven't yet seen the full enforcement focus from the government. The government has been mostly concerned with expeditiously getting aid to business of various sizes such that they have not truly pivoted to enforcement. The obvious cases are being spotted now; the more nuanced ones will take a while to come to the fore. I suspect that three to six months from now, we will see the first big wave of whistleblower allegations about alleged misuse of the federal relief that has been going out these past few months.

JB: Are there other aspects of the CARES Act that may lead to investigations, putting companies in a position of defending their interpretation of guidelines that are at once complex and vague?

MB: As Gejaa referenced, the CARES Act has led to financial institutions of all types to deliver enormous sums of money quickly to struggling businesses and individuals. This money was disbursed pursuant to regulations and other guidance that may be ambiguous, incomplete, unevenly administered, or subject to frequent amendment. As past precedent from the 2008 financial crisis shows, moreover, what seems clear now may turn out to be less clear later, especially as the political focus shifts from response to oversight and assessment.

One of the cornerstone programs of the CARES Act is the Paycheck Protection Program (PPP), which expands an existing loan guarantee program for eligible small businesses. Over the course of the PPP, which launched on April 3, Treasury has issued over twenty Interim Final Rules (IFRs), providing additional guidance on the PPP. In addition, the SBA has released ongoing guidance in its forty-nine Frequently Asked Questions (FAQs) related to PPP loans over the past few months, with the latest guidance issued on June 25.

CARES Act recipients should expect substantial second-guessing — especially with any widespread complications with or delays associated with CARES Act programs. Any investigations by PRAC, SIGPR, or existing oversight functions will culminate years later, when the political landscape may be entirely different, with little appreciation for the circumstances that exist today.

JB: With respect to the PPP, the government has indicated an intent to scrutinize PPP loans over $200,000. It has already started to file criminal charges against individuals who it says fraudulently applied for loans. Do you expect this to become a trend?

GG: What we are seeing in the early stages are the really egregious cases, cases that involve obvious alleged wrongdoing and that are blatant if true. There will be a significant amount of both civil and criminal enforcement down the road. The False Claims Act [FCA], which would apply to the program if there were fraud involved, is a statutory enforcement regime really driven by whistleblowers. These cases can be nuanced, and it can take a few months for these cases to be filed, analyzed, and result in formal investigations by DOJ. We will see more FCA and criminal investigations towards the later part of the year.

JB: Are companies coming forward to say they may have taken the funds when they didn't qualify?

GG: I know of some companies that have decided not to take the money or return it after careful thought about the qualification issue.

JB: Will the PPP program lead to investigations that extend beyond the PPP process?

GG: Any part of the response that involves federal money implicates government fraud enforcement regimes. And the response involves more than the PPP program, so we will see investigations that touch on various facets of the federal government's response.

JB: What kinds of evidence may be implicated?

GG: A lot of different types of evidence could be implicated, from financial records to email to instant messaging data to relevant mobile device data (texts, etc.).

JB: Let's turn to insider trading, which is under increased scrutiny from the SEC and DOJ as material non-public information — particularly related to impacts of COVID-19 — has impacted trading. Will there be any fallout for folks (members of Congress included) who traded stocks in companies that might benefit (or be harmed) from the COVID-19 stay-at-home orders prior to the orders being implemented? And do you anticipate insider-trading concern within companies as the financial impact continues to unfold?

MB: As seen in many new articles over the last few months, a few members of Congress reportedly traded stocks early in the COVID-19 outbreak

for significant returns. For instance, Senator Richard Burr reportedly is subject to a federal investigation for his stock sales on February 13.

Regulators have also explicitly stated that they are focusing their attention on insider trading risk. On March 20, Stephanie Avakian and Steven Peikin, the co-directors for the SEC's Enforcement Division, issued a public statement recognizing that in the present circumstances, the number of individuals with access to material nonpublic information may increase, and the value of such information will likely increase as well. The co-directors emphasized that individuals need to be mindful of their confidentiality obligations and the prohibitions on insider trading.

To mitigate potentially increased insider trading risk, companies may want to review their compliance programs to ensure appropriate communication regarding treatment of material nonpublic information. Companies also may want to consider whether any of their existing compliance controls relating to insider trading should be enhanced in light of the evolving workplace environment during COVID-19.

AM: There are real challenges with information control with remote working being the norm. Even as state stay at home orders are relaxed, many who have the ability to work from home are choosing to do so because we have figured out how to make it work and accepted a new normal. But having family members, including partners and adult children or parents sheltering together and sharing workspace means an increased risk for the spread of confidential information and the ability to trade on it. Of course being in close proximity, information sharing is more likely happening face to face so there may be more obstacles to the government satisfying their burden of proof without a data trail. That said, updated training and potential company investment in safeguards for work from home are smart steps, including making sure employees have a dedicated laptop for work with privacy screens and headsets for conference calls.

JB: Do you see boards or audit committees demonstrating as much interest as the government in ferreting out fraud or misbehavior? The DOJ has focused once again on compliance programs, providing updated guidance. Are you seeing renewed focus on compliance programs within companies?

AM: Absolutely. Boards are very focused on internal privacy and data security programs to protect companies from cyberattacks, which have been on the rise since the start of the pandemic facilitated by the rise in online shopping and delivery and the chaos of shifting to working at home. Hackers have exploited vulnerabilities emanating from the shift in operations. Boards have also been reading about and focused on avoiding price gouging investigations. Even if deemed without merit, the press from such investigations is disastrous.

GG: I certainly agree. I have recently done a lot of work helping boards scrutinize the compliance function of several companies, assessing their efficacy, resource levels and staffing. Those endeavors reflect efforts by these boards to insure that any fraud or misbehavior is identified and dealt with appropriately. A part of these assessments involves matching up the programs against the guidance that has come out of DOJ and other federal agencies.

MB: Our experience is similar. Diligent companies and boards have remained vigilant about their compliance programs in the face of COVID-19. Companies focus on reviewing and revising their compliance programs regularly as: 1) the failure to establish maintain an effective compliance program may render members of the Board of Directors liable for losses caused by non-compliance with the law; and 2) under the Federal Sentencing Guidelines, the existence of an effective compliance program is a consideration for prosecutors in determining how to treat a company suspected of wrongdoing.

In July, the DOJ Criminal Division and the SEC Enforcement Division published an update to their FCPA Resource Guide; and in June, DOJ updated its guidance on the Evaluation of Corporate Compliance Programs. The DOJ and SEC revisions to the FCPA Resource Guide include, for instance, language that focuses on whether a compliance program has adequate resources and is empowered to function effectively. The revisions are aligned with the DOJ and SEC's emphasis in the Guide on asking whether the compliance program has an established process for incorporating lessons learned both from its own and other similarly situated companies' experiences. [**Editor's Note**: See more on the updated guidance in "The Updated FCPA Resource Guide," in the September issue of *Business Crimes Bulletin*.] In other words, compliance programs must be refined and adapted over time in response to changing circumstances and based on new information.

Challenges from COVID-19 may present another layer of complexity for companies and boards to consider

when evaluating their compliance programs. As Amy noted, companies will likely need to determine whether additional risks arise from the business environment, including the remote work or modified in-person work environment.

JB: What do you suggest companies do to prepare for investigations?

GG: Data analytics can be a very effective tool to both monitor high risk areas and to identify areas for investigation. Key to such analytics is making sure that the compliance function has access to all the key data streams. I have seen some companies centralizing or warehousing data to support operational efficiency; a corollary benefit is that it helps compliance data monitoring as well.

AM: I agree with Gejaa. Last September, before COVID-19, former DOJ Deputy Assistant Attorney General Matt Miner called out in remarks posted on the DOJ website that the DOJ was increasingly using data analytics to identify indicators of healthcare fraud and was looking at whether companies that say they care about compliance — at least those involved in securities and commodities trading — were accessing their own data and using data analytics for compliance purposes. And we see new references to use of data analytics in the June 2019 updated DOJ guidance that Martine mentioned. The DOJ made clear that prosecutors will evaluate whether compliance personnel have the necessary access to data to monitor the effectiveness of a compliance program but will also check to make sure that such monitoring is actively taking place. Companies should be looking for opportunities to automate auditing and tracking with follow up for reports below minimum benchmarks.

JB: Natural drivers of fraud in 2020, as we've discussed, have been company and personal financial strain and – perhaps ironically – the large influx of government funds made available to business. Are there other vulnerabilities to which companies may be exposed that are leading to corporate or criminal investigations?

GG: There are. For example, a number of vaccines and numerous therapeutics in development and testing. Cyber threats are a significant issue, especially for companies involved in the life sciences industry in the COVID-19 response. Stealing intellectual property or personal health data from those trials is a real risk and we have already seen reports of efforts by state and non-state actors in that regard. In addition, there are also health privacy statutes, like HIPAA, that may be implicated; how patient data is handled (both in terms of security and use) by providers and life sciences companies is an area they should be carefully scrutinizing.

AM: Yes, and while companies are the victims of ransomware attacks or data breaches, there is increasing government focus on whether these attacks could have been prevented by reasonable security measures, creating additional investigative risk. This cyber-attack prevention is all the more complicated when businesses have switched to exclusive or almost exclusive working from home arrangements where new system vulnerabilities may have not been anticipated with the time pressures of moving to more virtual work. Expending the resources to do more fulsome systems analysis of data security vulnerabilities is critical for the long term as surges and the threat of a second wave of the pandemic continues.

MB: We expect that the staff at every government agency want to contribute to society's response to COVID-19. As one example, the SEC has expressed its intent to respond proactively to the impact of the coronavirus on capital markets and investors.

At the same time, risks to investors can become heightened during a market downturn, and we expect that the SEC's Enforcement Division will concentrate resources on certain types of investigations, including potential: 1) material misrepresentations and omissions about the impact of the coronavirus on public companies and investment products; 2) trading based on material nonpublic information about changes in the financial performance of public companies; 3) errors in the operation of trading platforms being stressed by high trading volume and volatility; 4) misuse of investor assets; and 5) frauds seeking to take advantage of investor anxiety. In the coming weeks and months, public companies should be vigilant regarding their disclosure practices and management of material, nonpublic information, and industry professionals similarly should be cautious when describing the impact of the pandemic on their investment services and products.

—❖—