October 2022

Day Pitney White Collar Roundup – October 2022 Edition

Preview of Coming Attractions on Corporate Criminal Enforcement

Almost like a trailer for a movie, Deputy Attorney General Lisa Monaco delivered remarks earlier this fall on the Department of Justice's (DOJ's) priorities in combating corporate crime, detailing what the DOJ is already doing and also, importantly, what may be on the horizon. The speech—accompanied by a memorandum outlining the Department's positions and goals—was delivered to a packed house at the NYU School of Law. Of the DOJ's priorities, number one is individual accountability. As Monaco made clear, "Whether wrongdoers are on the trading floor or in the C-Suite, we will hold those who break the law accountable, regardless of their position, status, or seniority." In terms of timing, the DOJ may focus on completing investigations and seeking criminal charges against individuals prior to or concurrently with entering into a resolution with the company. As a result, any undue or intentional delay in producing information or documents, particularly those that show individual culpability, may result in the reduction or denial of cooperation credit. Monaco's guidance next focused on companies with a history of misconduct. Prosecutors have been asked to approach corporate recidivism with renewed scrutiny, specifically taking into consideration the nature of the past misconduct and related circumstances, such as compliance programs and changes in corporate leadership. The DOJ will disfavor successive non-prosecution or deferred prosecution agreements with the same company. Indeed, Monaco delivered a warning: "If any corporation still thinks criminal resolutions can be priced in as the cost of doing business, we have a message—times have changed." Another DOJ focus, unsurprisingly, is the encouragement of voluntary self-disclosure. Noting the success of existing leniency programs for self-disclosure, including the Antitrust Division's Leniency Program, the voluntary disclosure program for FCPA violations, and the National Security Division's program for export control and sanctions violations, Monaco affirmed that it was the DOJ's goal to expand such programs across all of its divisions. She also reiterated the rewards: Absent aggravating factors, the DOJ "will not seek a guilty plea when a company has voluntarily self-disclosed, cooperated, and remediated misconduct." In addition, it will not require an independent compliance monitor "if, at the time of resolution, it also has implemented and tested an effective compliance program." Of course, how these policies and incentives are applied in particular cases is always challenging. Monaco finally addressed a fourth area of importance: greater uniformity and greater transparency in the selection of independent compliance monitors in appropriate cases, as well as prosecutors "monitoring the monitors" once in place. In connection with the speech, the DOJ released new guidance on initially identifying the need for a monitor, then selecting a monitor, and finally overseeing the monitor's work. These pronouncements, including the emphasis on individual responsibility, are certainly important in better understanding where the DOJ is likely to devote its time, attention, and considerable leverage. By the same token, and perhaps apropos of this Halloween season, the devil is usually in the details.

Popular E-Commerce Platform in Hot Water Over Data Security

New York Attorney General Letitia James recently set her sights on e-commerce giant Zoetop for its handling of large-scale customer data breaches. Zoetop owns the popular online clothing brands SHEIN and ROMWE, whose websites, as described in a press release and more detailed assurance of discontinuance published by James's office, were targeted by hackers who stole personal information from some 46 million consumers. While some may view Zoetop's earlier response as a lesson on how not to respond to data breaches, the Attorney General's findings and directives offer e-commerce platforms insights on how to minimize the risks of an enforcement action if their servers get hacked. In July 2018, as James's findings describe, Zoetop learned that hackers infiltrated its system and stole SHEIN customer account information. Zoetop's payment processor required Zoetop to engage a payment card industry-approved forensic investigator (PFI), and Zoetop also

independently engaged a cybersecurity firm to conduct investigations into the breach. The cybersecurity firm found that the hackers exfiltrated customer account information, including names, locations, email addresses, and passwords, but was unable to determine conclusively whether the hackers had actually stolen customer credit card information. Meanwhile, the PFI's investigation was incomplete because Zoetop did not provide the forensic investigator with access to the compromised systems and information about Zoetop's data security program. Despite its limited review, the PFI found Zoetop failed to comply with many of the regulations set forth in the Payment Card Industry Data Security Standard. Though Zoetop knew that more than 39 million SHEIN accounts were exposed, it issued a press release at the time stating that only about 6.4 million customers had been affected by the breach and contacted only a subset of them to recommend they initiate a password reset. Zoetop further misrepresented the severity of the breach by publicly stating that there was no evidence that credit card information was stolen. About two years later, in June 2020, Zoetop discovered that customer login credentials for a second site, ROMWE, were also stolen during the 2018 data breach and available for sale on the dark web. Zoetop reset the passwords of affected accounts but, as James's findings detailed, failed to notify customers that their credentials had been stolen. In September 2020, Zoetop also reset all SHEIN passwords impacted by the 2018 breach but did not inform customers of the reason for the reset. Later that year, Zoetop learned that additional ROMWE customer login credentials had been stolen, and ROMWE reset all passwords for accounts that existed at the time of the breach. Zoetop notified affected ROMWE U.S. customers by email and offered identity theft protection services. In total, nearly 7.3 million ROMWE account credentials were stolen. Given these events, the New York Attorney General's Office found that Zoetop failed to use reasonable measures to protect the data they collected from customers, identifying four areas in particular: password management, protection of sensitive customer information, monitoring, and incident response. It found that Zoetop violated New York Executive Law § 63(12) and General Business Law §§ 349 and 899-aa. In addition to a $1.9 million fine, Zoetop agreed to enhance its cybersecurity practices and report information related to its security and compliance practices to the office for a five-year period. Though some data breaches may be unavoidable, Zoetop's case offers good insights to e-commerce platforms on how to minimize the risks of enforcement action when breaches do occur. Among other things, businesses should be aware of all state-level data security laws that apply, ensure they are in compliance with applicable industry standards, and have a well-developed plan for prompt notification and remediation in place to utilize in the event of a breach.

Significant Changes to Financial Sanctions Guidelines Up and Running

This fall, the Financial Industry Regulatory Authority (FINRA) published Regulatory Notice 22-20 revealing significant revisions to its Sanction Guidelines ("Guidelines"), effective immediately. The Guidelines are utilized in FINRA appeals, disciplinary actions, and enforcement actions, and provide a range of sanctions and related factors to be considered by adjudicators for the particular securities violation at issue. Some key takeaways from the revisions are outlined below:

- Elimination of cap for serious violations: The revisions remove the upper limit of fine ranges for midsize and large firms in nine categories that FINRA has deemed the "most serious violations" it enforces. These categories are sales of unregistered securities, failure to respond truthfully in a FINRA investigation, best execution of trades, marking the open or close, churning or excessive trading, fraud and misrepresentations, excessive markups and commissions, certain systemic supervisory failures, and anti-money laundering (AML) violations.
- Creation of new fine ranges based on firm size: There are new fine ranges for small (1-150 registered representatives), midsize (151-499 representatives) and large firms (500 or more representatives). All fines—regardless of firm size—start at $5,000. Additionally, there are separate guidelines for fine ranges for individuals.
- Additional AML guidelines: Six additional guidelines emphasize the importance of AML compliance as described in FINRA's 2022 Exam Priorities. Further, there is no cap on fines for AML violations by midsize and large firms for failure to reasonably monitor and report suspicious transactions.
- New non-monetary sanctions: The Guidelines provide additional support for imposing non-monetary sanctions on repeat offenders and/or perpetrators of serious misconduct. Examples of non-monetary sanctions include suspending or barring a member firm from a particular business line or activity, requiring heightened supervision of certain individuals or departments, requiring a firm to retain an independent consultant to design and implement compliance improvements, and requiring a firm to certify it has revised supervisory procedures, among other things.

- Refocus and removal of select guidelines: Seven existing guidelines were revised to improve clarity and usability, and 20 others were deleted. Attachment A to the Regulatory Notice outlines those that were removed.

While adjudicators are not bound by the Guidelines, they provide important parameters for the resolution of FINRA actions and appeals; and with the comprehensive revisions revealed this fall, the Guidelines are likely to assume even greater significance. Firms would do well to study them closely, and given their immediate effectiveness, to do so now.

New FCA Settlements in the Sunshine and the Sooner States

The U.S. Attorney's Office for the Southern District of Florida recently announced that a home healthcare provider and two of its executives agreed to pay over $7 million for alleged violations of the False Claims Act (FCA). At the same time, the company reached a related settlement, including the payment of an almost $23 million fine, in the Western District of Oklahoma. As we described in an article earlier this year, the FCA allows the government to obtain civil recoveries from companies and individuals who knowingly submit false claims or misuse public funds. The FCA is one of the most powerful tools in the DOJ's arsenal, and in the previous full fiscal year, it obtained more than $5.6 billion in settlements and judgments from civil cases involving fraud and false claims against the government. Of the more than $5.6 billion in settlements, the vast majority—over $5 billion—involved the healthcare industry. And the recent and related resolutions in Florida and Oklahoma are no exception. Carter Healthcare is an Oklahoma-based home healthcare provider. As alleged in the DOJ's release in Florida, the company and its officers improperly billed the Medicare program for providing medically unnecessary therapy to Florida patients. The DOJ reaffirmed it is "committed to ensuring that providers bill only for appropriate procedures and amounts." In addition, the company's president and chief operations officer, Stanley Carter and Bradley Carter, respectively, agreed to be excluded from participation in all federal healthcare programs for five years. For its part, Carter Healthcare agreed to enter into a corporate integrity agreement requiring it to implement compliance improvements. Finally, because the FCA allows employees to file qui tam law suits on behalf of the government, the Carter Healthcare employees who acted as whistleblowers in the case received a substantial portion of the settlement. The same week, Carter Healthcare also agreed to pay an additional $22.9 million to resolve FCA allegations in Oklahoma. As alleged in the DOJ's release in Oklahoma, the company improperly compensated its home health medical directors in Oklahoma and Texas to induce patient referrals under the Medicare program and TRICARE, another government-sponsored health program. In addition, the company agreed to enter into a corporate integrity agreement with the U.S. Department of Health and Human Services, which requires an independent review of various arrangements made by or on behalf of Carter Healthcare entities. It also requires compliance-related certifications from key executives. In the article earlier this year linked above, we noted that the massive level of recoveries under the FCA, including those initiated by qui tam litigation, meant that participants in the healthcare industry should buckle up for a bumpy ride. The recent resolution of the Carter Healthcare cases across two states is but one of many examples.

Authors

Helen Harris
Partner

Stamford, CT | (203) 977-7418

hharris@daypitney.com

Naju R. Lathia
Partner

Parsippany, NJ | (973) 966-8082

nlathia@daypitney.com

Stanley A. Twardy, Jr.
Of Counsel

Stamford, CT | (203) 977-7368

satwardy@daypitney.com