October 9, 2017

White Collar Roundup - October 2017

SEC Chair Outlines Cyber Risks Including EDGAR Hack

In a Statement on Cybersecurity, Securities and Exchange Commission (SEC) Chair Jay Clayton described the SEC's involvement with and approach to cybersecurity and related incidents. He began, "Data collection, storage, analysis, availability and protection (including security, validation and recovery) have become fundamental to the function and performance of our capital markets, the individuals and entities that participate in those markets, and the [SEC]." Further, he noted the SEC "is focused on identifying and managing cybersecurity risks and ensuring that market participants – including issuers, intermediaries, investors and government authorities – are actively and effectively engaged in this effort and are appropriately informing investors and other market participants of these risks." The statement also detailed the SEC's internal cybersecurity challenges, including its investigation into attacks on its EDGAR system in which the SEC saw "cyber threat actors attempting to compromise the credentials of authorized users, gain unauthorized access to filings data, place fraudulent filings on the system, and prevent the public from accessing our system through denial of service attacks." And, it appears, the incident the SEC detected in 2016 might have been used in August 2017 to provide the basis for illicit gain through trading. The statement then turns to the SEC's cybersecurity goals in the coming years, including its "objective to contribute substantively to a financial market system that recognizes and addresses cybersecurity risks and, in circumstances in which these risks materialize, exhibits strong mitigation and resiliency."

SDNY's Full-Court Press on College Basketball

Joon H. Kim, the Acting U.S. Attorney for the Southern District of New York, announced the arrest of 10 individuals, including four Division I NCAA men's basketball coaches and senior executives at a major athletic apparel company, charging them with two fraud and corruption schemes. The government alleges that in the first scheme, college basketball coaches took bribes from athlete advisors to influence their players to use the services of the advisors paying the bribes. It alleges that the second scheme involved a senior executive at the apparel company funneling bribe payments to high-school-aged players and their families to secure commitments to attend universities sponsored by the company. The charges include wire fraud, bribery, Travel Act violations and conspiracy. Kim said, "The picture of college basketball painted by the charges is not a pretty one – coaches at some of the nation's top programs taking cash bribes, managers and advisors circling blue-chip prospects like coyotes, and employees of a global sportswear company funneling cash to families of high school recruits."

FOIA Battle Over Monitorship Reports

Back in 2008, Siemens AG entered into a deferred-prosecution agreement (DPA) with the U.S. Department of Justice (DOJ) regarding its involvement in a Foreign Corrupt Practices Act scheme in Argentina, Bangladesh, Venezuela and Iraq. As part of that DPA, Siemens agreed to a corporate monitor, who would report to the DOJ regarding Siemens' compliance with the terms of the DPA. The news outlet 100Reporters filed requests under the Freedom of Information Act (FOIA) to obtain reports and other information about compliance reforms at Siemens, including reports from the monitor to the DOJ. The DOJ refused to provide them, and 100Reporters sued in the U.S. District Court for the District of Columbia. U.S. District Judge Rudolph Contreras ruled in March that the DOJ had properly exempted some material but that some could be disclosed. The DOJ filed for summary judgment and argued that disclosing the information sought would "decrease the amount and accuracy of information that DOJ receives from future monitorships, which will ultimately inhibit DOJ's ability to reduce corporate crime." For more, click here.

False Claims Act's Materiality Standard Strikes Again

The "rigorous" materiality requirement in False Claims Act cases post *Universal Health Servs., Inc. v. United States ex rel. Escobar* just cost a relator millions of dollars. The U.S. Court of Appeals for the Fifth Circuit recently vacated a $663 million False Claims Act verdict in *United States of America ex. rel. Harman v. Trinity Industries Inc.* The court found the fraud allegations could not stand because materiality was lacking. In *Harman*, the government did not intervene in the relator's case and even gave a pretrial statement supporting the defendant, Trinity. Nevertheless, the jury found the government had been defrauded and awarded Joshua Harman $663 million. The Fifth Circuit noted the case should never have made it to the jury because the materiality standard for the falsity to the government was not met.

Briefing to Supreme Court Explores the Scope of Cell Site Searches

This term, the U.S. Supreme Court will hear *Carpenter v. United States*, which addresses whether law-enforcement officers must obtain a warrant to collect historical cellphone location information. Carpenter filed his brief earlier this summer, and the government responded last month. Carpenter argues the Stored Communications Act and the Fourth Amendment require the government to obtain probable-cause warrants to obtain that information instead of mere subpoenas to the cellphone carriers. In response, the government argues individuals can't claim any right to privacy under the Fourth Amendment because they provide that information to third parties, notably their cellphone carriers. "Cellphone users voluntarily reveal to their providers information about their proximity to cell towers so the providers can connect their calls," the government argued. "Users cannot reasonably expect that the providers will not reveal that business information to the government."

Beware the Ever More Creative E-mail Scam

As has been widely reported, the president's son-in-law and advisor Jared Kushner has retained counsel to assist him with the investigation of Independent Counsel Robert Muller. His lawyer, Abbe Lowell, was apparently duped into responding to e-mails that purportedly came from Kushner but actually came from a prankster. Those e-mails, which came from an e-mail address that was not Kushner's, asked Lowell whether he – meaning Kushner – could lawfully delete e-mails that contained adult content. Lowell responded, "Don't delete. Don't send to anyone. Let's chat in a bit." Fortunately, that advice was sound, but this incident reveals yet again the importance of being ever vigilant when dealing with e-mails and other electronic communications. For more, click here.

Perils of Getting Your Plea Back

Criminal defendants face a stark choice: go to trial or plead guilty. Often, especially in white-collar cases, defendants find themselves willing to admit they did something wrong, but have a difficult time admitting they did what the government alleges against them. Such was apparently the case in *United States v. Khazaee*, in which the defendant was accused of violating the Arms Export Control Act and agreed to plead guilty. The plea hearing was a rough one in which the district court allowed the defendant an 80-minute break to discuss with his lawyer whether he truly did want to plead guilty. Ultimately, he did so. But on appeal, he sought to withdraw his plea. At oral argument at the Second Circuit (available here), Judge John Walker suggested Khazaee might "rue the day" if he were allowed to withdraw his plea because of the extent of the government's allegations against him. Whether the Second Circuit allows him to withdraw his plea is still to be determined, but if it does, then he will undoubtedly face a trial that might not turn out as he hopes. Only time will tell.

Authors



Helen Harris
Partner

Stamford, CT | (203) 977-7418

hharris@daypitney.com



Stanley A. Twardy, Jr.
Of Counsel

Stamford, CT | (203) 977-7368

satwardy@daypitney.com