June 7, 2017

White Collar Roundup - June 2017

Hard Charging: Sessions Issues New Policy

U.S. Attorney General Jeff Sessions issued a Memorandum for All Federal Prosecutors to outline the charging and sentencing policy of the U.S. Department of Justice (DOJ). The policy notes the DOJ's responsibility to fulfill its "role in a way that accords with the law, advances public safety and promotes respect for our legal system." The memorandum then sets forth "simple but important" directives. First, it directs prosecutors to "charge and pursue the most serious, readily provable offense," which "affirms our responsibility to enforce the law, is moral and just, and produces consistency." The memorandum directs prosecutors to "fully utilize the tools Congress has given us" and notes "the most serious offenses are those that carry the most substantial guidelines sentence, including mandatory minimum sentences." It also recognizes there "will be circumstances in which good judgment would lead a prosecutor to conclude a strict application of the above charging policy is not warranted. In that case, prosecutors should carefully consider whether an exception may be justified." And when such departure from the charging policy is considered, the decision "must be approved by a United States Attorney or Assistant Attorney General, or a supervisor designated by the United States Attorney or Assistant Attorney General, and the reasons must be documented in the file." Second, it directs prosecutors to "disclose to the sentencing court all the facts that impact the sentencing guidelines or mandatory minimum sentences, and should in all cases seek a reasonable sentence under the factors in 18 U.S.C. §3553." It notes that usually "recommending a sentence within the advisory guideline range will be appropriate" and that any recommendation for a departure or variance will "require supervisory approval, and the reasoning must be documented in the file."

President Orders Federal Agencies to Strengthen Cybersecurity

President Donald Trump issued an executive order regarding cybersecurity issues. The order contains three policy statements as well as directives to implement those policies. The first policy statement emphasizes that the "executive branch operates its information technology (IT) on behalf of the American people" and reasons that its "IT and data should be secured responsibly using all United States government capabilities." As a result, the "President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises." Further, the order states, "because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch." Among other things, agencies are required within 90 days to submit a "risk management report" in accordance with the Framework for Improving Critical Infrastructure Cybersecurity, developed by the National Institute of Standards and Technology (NIST), and to manage cyber-risk going forward pursuant to the NIST framework. The second policy statement requires the executive branch to use "its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the nation's critical infrastructure." The third policy statement relates to cybersecurity's importance to the economy. It states the executive branch will "promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft." It also emphasizes the administration's promise "to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace."

ABA Cautions Lawyers to Secure Their E-mail Correspondence

The Standing Committee on Ethics and Professional Responsibility of the American Bar Association (ABA) issued Formal Opinion 477, "Securing Communication of Protected Client Information." (If you are wondering whether ABA ethics opinions are really white collar matters, you might note, as the opinion itself does, that a lot of mischief, including white collar mischief, results from the bad guys obtaining such information.) Back in 1999, the ABA issued Formal Opinion 99-413, which explained

that lawyers "have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the internet, despite some risk of interception and disclosure." But that, of course, was in 1999. It's now 2017, and the incidents of hacking and disclosure of confidential information have skyrocketed. As a result, the ABA issued Formal Opinion 477 to bring its view of using e-mail up to date. It notes that in the "technological landscape of Opinion 99-413 …unencrypted email posed no greater risk of interception or disclosure than other nonelectronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication." But (and this is a big "but") it reasons that "cyberthreats and the proliferation of electronic communications devices have changed the landscape, and it is not always reasonable to rely on the use of unencrypted email." It concludes that "lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters" and, applying the factors set forth in Comment 18 of Model Rule of Professional Conduct 1.6, "to determine what effort is reasonable." The opinion then sets forth several considerations to aid in that effort.

ACLU Looking for Information About Cell-Site Simulators

The American Civil Liberties Union (ACLU) filed a Freedom of Information Act (FOIA) request to both U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) regarding their use of cell-site simulators to enforce immigration laws. Cell-site simulators precisely locate a target mobile phone by, among other things, contacting it in the guise of one or more towers of the user's mobile service provider. As we reported here and detailed here, law enforcement has turned to the use of these simulators to find and apprehend targets of criminal investigations or subjects of arrest warrants. We noted that courts are cautious about endorsing the wide use of such equipment, which have potential implications under the Fourth Amendment. In its FOIA request, the ACLU notes that although "it has been publicly known for several years that ICE has purchased cell-site simulator technology," a recent report in the Detroit News about an ICE search warrant was "the first time the ACLU has seen evidence of use of the technology in a particular ICE investigation or operation." The ACLU notes that although the Department of Homeland Security had previously issued a policy directive governing use of cell-site simulators, "little is publicly known" about their use by ICE and CBP. The ACLU requested 10 categories of records to flesh out the use of such equipment by both agencies. It also requested expedited processing of its request. ICE may be contemplating its response to the ACLU, but it also will have to consider how to respond to a letter from Sen. Ron Wyden, D-Ore., which requests similar information from ICE.

DeCinces Is Convicted

As we reported here, former Major League Baseball player Douglas DeCinces was indicted for insider trading. The trial court had granted a motion in limine to exclude certain evidence in the case, but the U.S. Court of Appeals for the Ninth Circuit reversed and remanded. The trial began earlier this year and, after almost two months, resulted in a jury convicting DeCinces of 14 counts of insider trading. It hung on the other 18 counts and the judge declared a mistrial on them. According to the government's press release, the trial evidence showed DeCinces purchased stock in Advanced Medical Optics Inc. (NYSE: EYE) after obtaining confidential information that the company was about to be acquired by Abbott Laboratories. According to the government, DeCinces "purchased a total of 90,700 shares of EYE stock, which he sold soon after Abbott's tender offer for the company was publicly announced, and realized approximately $1.3 million in profits." David Parker, who obtained the insider information from DeCinces, was also convicted. But the jury was unable to reach a verdict regarding the insider-trading charges against James Mazzo, CEO of Advanced Medical Optics and DeCinces' neighbor, who the government alleged provided the insider information to DeCinces. The court declared a mistrial on those charges, which remain pending against Mazzo.

Another Conviction for Fraud Involving Municipal Bonds

We reported here that N. Aaron Troodler, former executive director of Ramapo Local Development Corp. (RLDC), pleaded guilty to participating in securities fraud and wire fraud regarding the municipal bonds issued by RLDC and the town of Ramapo. Christopher St. Lawrence, the Ramapo town supervisor and Troodler's alleged partner in the scheme, was also convicted by a jury of 20 counts of conspiracy, securities fraud and wire fraud. In the press release announcing the conviction, Joon H. Kim, acting U.S. attorney for the Southern District of New York, said, "As the jury found today after trial, Christopher St. Lawrence lied repeatedly to the investing public about the state of Ramapo's finances. The integrity of the

$3.7 trillion municipal bond market is of critical importance to both investors and municipalities that rely on this market. The verdict today, in a case of public corruption meets securities fraud, stands as a victory for both honest government and fair financial markets."

Authors

Helen Harris
Partner

Stamford, CT | (203) 977-7418

hharris@daypitney.com

Mark Salah Morgan
Partner

Parsippany, NJ | (973) 966-8067

New York, NY | (212) 297-2421

mmorgan@daypitney.com

Stanley A. Twardy, Jr.
Of Counsel

Stamford, CT | (203) 977-7368

satwardy@daypitney.com