May 6, 2019

White Collar Roundup - May 2019

SEC Issues Privacy Risk Alert to Registrants

In a sign of its own deepened recognition of the risk of identity theft and other compromise of personal information, the Securities and Exchange Commission (SEC) has put registered firms on further notice that many need to substantially improve their cybersecurity and related controls. On April 16, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert. Notwithstanding that document's anodyne title (*Investments Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies*), OCIE's message was pretty pointed. In four concise pages, OCIE summarized what it characterized as the "most common deficiencies or weaknesses" detected in recent examinations assessing compliance with Reg. S-P, the SEC implementation of the Gramm-Leach-Bliley Act's privacy requirements. OCIE found that registrants had failed to adopt fundamental protections, including written customer information safeguards, inventories of customer information storage locations and plans to govern cybersecurity incident response. In addition, OCIE found serious training deficiencies, such as an absence of controls to limit transmission of customer information over personal devices or to revoke logon rights of departing staff. Moreover, the Risk Alert contained a knowing and well-placed shot that condemned halfhearted (or less) protections, such as "written policies and procedures that contained numerous blank spaces" that were designed to be filled in by registrants" —but hadn't. How the SEC will respond if these defects persist remains to be seen. It's fair to say, however, that regulators are giving the problem tougher scrutiny than ever before.

Investment Advisers or Ponzi Schemers?

The owner and two former directors of the Woodbridge Group of Companies, LLC, were charged with "orchestrating a massive investment fraud (*Ponzi*) scheme" by the U.S. Attorney's Office for the Southern District of Florida, according to a press release. The indictment alleges that these individuals made material misrepresentations and operated a kind of "boiler room," featuring "high-pressure sales tactics, deception, material misrepresentations, and investor manipulation" in the course of the scheme. "Through telemarketing, Woodbridge sales agents contacted potential investors located throughout the United States, and solicited, offered, and sold Woodbridge investments to them. For the fraud-based investments, the defendants and their co-conspirators' main business model was to solicit money from investors and, in exchange, issue investors promissory notes reflecting purported loans to Woodbridge that paid monthly interest and matured in twelve to eighteen months. The defendants claimed that the investments were tied to real property owned by third-party property owners." According to the press release, "[a]t least 2,600 of these investor victims invested their retirement savings, totaling approximately $400 million."

Wire Act and Lotteries

A New Hampshire federal judge denied the request of the U.S. Department of Justice (DOJ) to dismiss the New Hampshire Lottery's suit for its reinterpretation of the Wire Act. According to this news report, "the New Hampshire Lottery Commission filed a lawsuit seeking to have the judicial branch overrule the Office of Legal Counsel opinion and declare lotteries exempt

from the Wire Act." The DOJ pushed back, seeking "to have the lawsuit dismissed, arguing that it had no intention at this time of bringing legal action against New Hampshire." It appears that the judge was frustrated with the case. He "called the original 1961 statute a 'mess'" and suggested that the matter might end up at the U.S. Supreme Court. And as reported here, the DOJ tried to strengthen its hand in the litigation by releasing a memo to all federal prosecutors, noting that the opinion that reinterpreted the Wire Act "did not address whether the Wire Act applies to State lotteries and their vendors." It further noted, "The Department is now reviewing that question. Department of Justice attorneys should refrain from applying [the Wire Act] to State lotteries and their vendors, if they are operating as authorized by State law, until the Department concludes its review."

SDNY Steps Up Attack on Opioid Distribution

Geoffrey S. Berman, U.S. Attorney for the Southern District of New York, and Ray Donovan, the Special Agent in Charge of the New York Division of the U.S. Drug Enforcement Administration (DEA), announced felony charges against Rochester Drug Co-Operative, Inc. (RDC), which is one of the 10 largest pharmaceutical distributors in the United States. According to the announcement, the company and its former chief executive officer and chief compliance officer were charged with unlawfully distributing oxycodone and fentanyl and conspiring to defraud the DEA. RDC also entered into a consent decree in which it agreed "to accept responsibility for its conduct by making admissions and stipulating to the accuracy of an extensive Statement of Facts, pay a $20 million penalty, reform and enhance its Controlled Substances Act compliance program, and submit to supervision by an independent monitor." The company also entered into a deferred prosecution agreement, which has a five-year term. U.S. Attorney Berman made plain the nature of this action, saying, "This prosecution is the first of its kind: executives of a pharmaceutical distributor and the distributor itself have been charged with drug trafficking, trafficking the same drugs that are fueling the opioid epidemic that is ravaging this country. Our Office will do everything in its power to combat this epidemic, from street-level dealers to the executives who illegally distribute drugs from their boardrooms."

Suppression at Second Circuit

The U.S. Court of Appeals for the Second Circuit in *United States v. Durand* remanded the prosecution of Jacques Durand for a suppression hearing regarding inculpatory statements that were used against him at trial. The case relates to an investigation by the U.S. Postal Investigation Service in the winter of 2014 into complaints of mail theft and identity fraud in Queens. During the course of the investigation, inspectors began to focus their attention on phone numbers that were used to call banks about fraudulent credit card accounts. The inspectors thought that if they "could link a person to one of the telephone numbers they identified as connected to the fraudulent accounts, then they could likely identify the person obtaining the fraudulent credit cards." In that vein, they created a list of five or six telephone numbers of interest. Their attention then turned toward Durand, whom they handcuffed and brought to an interrogation room. Without providing *Miranda* warnings, they asked him for his Social Security number, his address, his employment status and his telephone number. Durand bristled at providing the telephone number, but ultimately did so. They called the number, and Durand's cell phone rang. The inspectors then Mirandized Durand, and he requested an attorney. He moved to suppress the identification of his phone number, arguing that it was provided in violation of *Miranda*. The district court denied the motion to suppress, concluding that it was unnecessary to hold a hearing because the phone number was simply "pedigree information" for which no *Miranda* warnings are required. Ultimately, Durand was convicted based, in large part, on his phone number's connection to the fraud. He appealed, and the Second Circuit remanded for a suppression hearing. It noted that it has previously "explained that an officer cannot ask a pedigree question even if it otherwise might fall within the booking exception, if she knows or should have known the question was reasonably likely to elicit an incriminating response." The court noted that if on remand the district court concludes suppression is appropriate, it should vacate the conviction and hold a new trial without that evidence; if not, then the conviction may stand.

Microsoft Discloses Insider Threat to Cybersecurity

Cybersecurity threats aren't just from phishing attacks. As reported here, Microsoft has disclosed that the credentials of an Outlook.com support agent had been compromised, which opened access to an unknown number of Outlook accounts. According to a Microsoft e-mail, "Our data indicates that account-related information (but not the content of any e-mails) could have been viewed, but Microsoft has no indication why that information was viewed or how it may have been used." Experts term this type of breach an "insider threat" because hackers get access to a user's information by obtaining the credentials of an employee or contractor of the service provider. Another difficulty is the service provider's ability to identify the breach; after all, it is not their systems that the hacker is accessing, but the systems of their customers. As a result, it's less likely that the service provider will become aware of the breach.

SCOTUS Orders Shorter Briefs

The U.S. Supreme Court announced new rules regarding the length of merits briefs, beginning on July 1. Noting that many litigants provide briefs that are under the current 15,000 word limit, the Court decided to shorten the length for merits briefs (for petitioners and respondents) to 13,000 words. It also imposed a new deadline for reply briefs, to give the Court more time to review them before argument. Given this action, lower courts might similarly change their word limits to follow the shorter-is-better trend. Only time will tell. For more, click here.

Would you like to receive our *White Collar Roundup* newsletter? Sign up here.

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