April 3, 2017

White Collar Roundup - April 2017

U.S. Department of Justice Extends Its FCPA "Pilot Program"

The U.S. Department of Justice (DOJ) launched the so-called Pilot Program in April 2016 to "promote greater accountability for individuals and companies that engage in corporate crime by motivating companies to voluntarily self-disclose [Foreign Corrupt Practices Act]-related misconduct, fully cooperate..., and, where appropriate, remediate flaws in their controls and compliance programs." To review the original announcement and documents, click here. Following the resolution of several FCPA investigations pursuant to the Pilot Program in 2016, the program was due to expire on April 5. But Acting Assistant Attorney General Kenneth A. Blanco announced during a speech at the American Bar Association's National Institute on White Collar Crime that the DOJ would continue with the Pilot Program for the time being. He said that when the Pilot Program expires, DOJ will review its "utility and efficacy" to determine "whether to extend it, and what revisions, if any, [DOJ] should make to it." He also said, "The program will continue in full force until we reach a final decision on those issues." To read about Blanco's announcement, click here.

DOJ Persists – And So Far Prevails – in Two New Warrant Applications for Users' Content Stored Abroad

The government's clash with providers of electronic communication services continues, with the government seeming to have the upper hand in the newest skirmishes. In criminal investigations, the government has long invoked the Stored Communications Act (SCA) to obtain search warrants requiring the providers to disclose e-mail and other content that they've stored abroad. But in July 2016, a Second Circuit panel ruled in favor of Microsoft, holding it unreasonable to construe that the SCA supplies extraterritorial authority when it contains no express provisions on that score. Moreover, as we reported here, an evenly split en banc panel denied the government's petition for rehearing, with four judges sharply dissenting. In the meantime, however, two courts elsewhere have preliminarily adopted the dissenters' views. In *In re Search Warrant No. 16-1061-M to Google*, venued in the Eastern District of Pennsylvania, Google is trying to persuade a district judge to overturn Magistrate Judge Thomas J. Rueter's February order compelling disclosure of content wherever stored, including overseas. In that order, echoing the Second Circuit dissenters, Magistrate Judge Rueter held that a warrant that requires a provider from within the United States to search for and copy content stored abroad does not involve an extraterritorial search or seizure. Accordingly, no additional authority is required under the SCA or other statute. In the alternative, Magistrate Judge Rueter held that it would be unreasonable to construe the SCA to lack extraterritorial reach. He reasoned that because Google's algorithms unpredictably shift data storage from country to country, the retrieval of data by requests to the host country by multilateral legal assistance treaty would be impossible. In another ongoing case, *In re: Two email accounts stored at Google, Inc., No. 17-M-01235*, venued in the Eastern District of Wisconsin, Google has moved to amend the search warrant to delete the requirement to produce content stored overseas. In his order resolving the motion, Magistrate Judge William E. Duffin squarely endorsed the view of the four Second Circuit dissenters who had favored en banc review: "Provided the service provider is within the reach of the court, the court may lawfully order that service provider to disclose data in the provider's custody or control, without regard of where [*sic*] the provider might choose to store the ones and zeros that comprise the relevant data."

Prepaid Restitution Yields Little Benefit

In *United States v. Bodouva*, the Second Circuit trampled defendant Christine Bodouva's dream of not owing forfeiture due to her pre-sentencing payment of restitution in her criminal prosecution. Bodouva had been caught embezzling from her company's 401(k) plan to the tune of $127,854.22. After her indictment, but before her trial, she paid $126,979.63 back to the 401(k) plan she allegedly purloined. She was convicted by a jury and urged the sentencing court to reduce the amount of

forfeiture it imposed by the amount she repaid to the 401(k) plan. The district court determined it had no statutory authority to do so and ordered forfeiture of the full amount. Bodouva appealed, and the Second Circuit affirmed. It first noted that the statutory purposes for forfeiture and restitution are different. Forfeiture is designed to punish the defendant by taking her ill-gotten gains to ensure that her crime does not pay. Restitution, on the other hand, is designed to make the victim of her crime whole by returning to it any money taken in the scheme. The court canvassed the forfeiture statutes and explained that "Congress provided for reductions in forfeiture amounts resembling the offset requested here, but only in certain circumstances." And unfortunately for Bodouva, payment of restitution is not one of those circumstances. Therefore, the court concluded, the district court had no statutory authority to reduce the amount of forfeiture ordered and correctly refused to do so.

Cybersecurity Disclosure Might Become Law

Senators Jack Reed (D-R.I.), Susan Collins (R-Maine), and Mark Warner (D-Va) introduced Senate Bill 536, titled the "Cybersecurity Disclosure Act of 2017." The bill is designed "to promote transparency in the oversight of cybersecurity risks at publicly traded companies." It requires that the Securities and Exchange Commission (SEC) issue rules within a year that require registrants "to disclose whether any member of the governing body, such as the board of directors or general partner, of the reporting company has expertise or experience in cybersecurity" with details of that experience. If any registrant has no such expertise or experience, it must "describe what other cybersecurity steps taken by the reporting company were taken into account" by those responsible for identifying and evaluating nominees for the company's governing body. The bill further directs the SEC to consult with the National Institute of Standards and Technology (NIST) to "define what constitutes expertise or experience in cybersecurity." Specifically, the focus should be on "professional qualifications to administer information security program functions or experience detecting, preventing, mitigating or addressing cybersecurity threats," consistent with NIST Special Publication 800–181.

Muni-Bonds: A $3.7 Trillion Industry Ripe for Criminal Prosecution

Before leaving office, Southern District of New York U.S. Attorney Preet Bharara announced the guilty plea of N. Aaron Troodler, former executive director of the Ramapo Local Development Corporation (RLDC). Bharara asserted that Troodler "defrauded both the citizens of Ramapo and thousands of investors around the country, helping to sell over $150 million of municipal bonds on fabricated financials." Troodler pleaded guilty and admitted to committing securities fraud. Bharara continued, "This guilty plea, in what we believe to be the first municipal bond-related criminal securities fraud prosecution, is a big step in policing and bringing accountability to the $3.7 trillion municipal bond market." The information alleged that Troodler and others misrepresented the finances of the Town of Ramapo, "in order to conceal the deteriorating state of the Town's finances and the inability of the RLDC to make scheduled payments of principal and interest to the holders of its bonds from its own money." Troodler agreed that he lied to investors by "making up" false assets in the Town's general fund, which is its primary operating fund. He also lied to the "RLDC's bond rating service" and inflated the general fund with a "fake receivable." Troodler's sentencing is scheduled for September 18.

Prominent Twitter Accounts Hacked to Spread Hate Speech

Twitter accounts for several individuals as well as various organizations, such as Forbes, Amnesty International, and BBC News, recently began tweeting swastikas and other Nazi-related messages. According to this article, the hacking is thought to be related to Turkey's diplomatic spat with the Netherlands and Germany. The various victims re-gained control of their accounts, but it appears the accounts were compromised by an attack on the third-party service, Twitter Counter. Both Twitter Counter and Twitter are investigating the matter. Cybersecurity experts urge users of Twitter to review their passwords and the permissions granted to third-party apps and services to help limit the risk of future compromises. To read more, click here and here.

Convicted Congressman Charges Government with Hiding Evidence

Former Arizona Congressman Rick Renzi argued for a new trial before the U.S. Court of Appeals for the Ninth Circuit. His claim? That he only recently learned that the Federal Bureau of Investigation (FBI) had promised to pay the government's cooperating witness $25,000 for his cooperation. At Renzi's trial, investor Philip Aries testified about his involvement with Renzi in a land deal, which the government claimed was part of Renzi's scheme to use his office to enrich himself. Renzi argued that the government had an obligation to disclose the compensation and that its failure to do so justifies a new trial.

Renzi claims the government invoked Aries' testimony 90 times during its closing and asserted that Aries hadn't received "one thin dime" for his cooperation. But it turns out that weeks before Renzi's cert. petition to the Supreme Court was denied, Aries e-mailed the lead prosecutor to obtain his $25,000 payment for his testimony. Upon receiving this e-mail, the prosecutor notified the defendant. Renzi's attorney argued to the Ninth Circuit, "Had Mr. Aries sent the same email to the prosecutor after the decision, the government presumably would have paid him his reward by now, as the agents had planned all along, and the defense never would have known a thing, which is what the government had intended. We never would have known that in November 2006 the FBI coaxed Mr. Aries into continuing to cooperate by ... telling him that recording calls was exactly the sort of thing that the FBI rewarded. We never would have known that the lead AUSA reviewed admonishments just before trial, forms that the district court found clearly contemplated payments to witnesses, and decided not to give them to defense." Unsurprisingly, the government disagreed and minimized the importance of Aries' testimony at the trial. To watch a video of the argument, click here.

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