April 6, 2018

White Collar Roundup - April 2018

Deputy Attorney General Sets the Stage for White Collar Crime Enforcement

On the last day of the American Bar Association's National Institute on White Collar Crime, Deputy Attorney General Rod Rosenstein described some of the white collar crime priorities of the Department of Justice in the coming year. After highlighting recent prosecutions for Medicare and Medicaid fraud, military procurement fraud, and illegal offshore tax shelters, Rosenstein intimated that the DOJ will have "more such cases in the future." He also lauded the work of the Environmental Crimes Unit, which has prosecuted "perpetrators of fraudulent transactions involving tax credits for renewable fuels." And he stressed that the DOJ's "white collar enforcement is also becoming smarter and more efficient thanks to the use of technology," including the use of "sophisticated data analytics in a number of the Department's major health care fraud cases." He said the DOJ is "using analytics to more quickly identify, investigate and prosecute manipulation of the securities markets, and other forms of fraud that threaten the integrity of America's financial system." Finally, he noted the DOJ's "ability to adapt to the types of criminal conduct normally described as 'white collar,'" including drug trafficking and national security investigations, which "frequently involve sophisticated data analysis and complex financial transactions."

Shkreli's Antics, and an Unusual but Perhaps Effective Defense Tack

On March 9, in Brooklyn federal court, District Judge Kiyo Matsumoto sentenced Martin Shkreli, 35, following his conviction at trial on charges of defrauding investors in his hedge funds and manipulating the stock price of a pharmaceutical company. The court imposed a prison term of seven years and forfeiture in excess of $7.3 million. For a white collar defendant, this was a stiff sentence. The sentence might have been harsher still but for shrewd argument by defense counsel Benjamin Brafman, aimed at tempering fallout from Shkreli's many prior outrageous but uncharged antics. Even before indictment, Shkreli was notorious for having raised the price of a rare, lifesaving drug by 5,000 percent. Pretrial, Shkreli live-streamed monologues from his home mocking both the charges against him and the assigned prosecutors to boot. Before the jury, he alternately rolled his eyes and read a chemistry textbook. Post-trial, Shkreli publicly offered $5,000 to anyone who would deliver to him a hair plucked from Hillary Clinton's head (whereupon the court revoked bail). All this (and more) prompted Brafman at sentencing to adopt an unusually frank parental tone. "I'm old enough to be his father," said Brafman. "There are times when I want to hug and hold him, times I want to punch him in the face for some of the things he's said. ... Quite frankly, I've got my begging voice on." This unorthodox approach may have worked—the seven-year sentence imposed by Judge Matsumoto was eight years less than prosecutors had urged.

The Stored Communications Act, a Cruise Ship and Continued Confusion

The outmoded federal Stored Communications Act (SCA) continues to breed confusion. Latest problem: how—if at all—the SCA applies to WiFi service that an enterprise offers to customers as an amenity to its core business (customer WiFi). The SCA establishes ground rules for the government's acquisition in criminal investigations of data relating to customers of "electronic communications service" (ECS) and "remote computing service" (RCS). The most basic customer account ID data is available by mere subpoena. As to anything else, including usage data, the SCA requires prosecutors to demonstrate, at minimum, relevance and materiality to an ongoing investigation. While the SCA uses broad terms to define what ECS and RCS entail, Congress enacted this law well before customer WiFi and other communications amenities came into common usage—which brings us to a recent case in federal court in the District of Columbia. Last summer, federal prosecutors sought to identify who had initiated fraudulent bank wire transfers using customer WiFi onboard a Royal Caribbean cruise ship. The prosecutors applied under the SCA for an order directing the cruise line, as an ECS provider, to produce logs relating to several Internet sessions. A magistrate judge pushed back, ultimately holding that the court lacked authority under the SCA. That court reasoned that Royal Caribbean could not be an ECS provider, as that would also mean—as Congress could not

possibly have intended—that the SCA's ambit extends even to *free* customer WiFi systems. Last month, a district judge reversed the magistrate judge, ordering Royal Caribbean to produce its own logs and those of its vendors. In holding that Royal Caribbean is an ECS provider subject to the SCA, the March 8 opinion emphasized the complex shipboard, satellite and Internet system at issue, the fact that Royal Caribbean charged passengers for access, and the court's view that the government's request was narrowly "focused." This approach left much unresolved. Customer WiFi at many businesses (e.g., hotels and restaurants) is far less sophisticated than the cruise line's. It also is often free of charge. Moreover, whether a government request for data is sufficiently focused is something defendants and their counsel can contest (and now surely will). Thus, the most salient impact of the March 8 opinion may be its holding that even though the vendors were themselves ECS providers, the government was still entitled to saddle Royal Caribbean with the burden of producing the vendors' logs too. Will this rationale apply to planes, trains and automobiles as well? We'll see.

The SCA and (Some) New Clarity From Congress

Last month, the SCA got a small update. On March 23, tucked away in the massive budget bill, Congress passed the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act). The CLOUD Act is an attempt to solve issues underlying long-running litigation between federal law enforcement and Microsoft Corporation. The U.S. Supreme Court heard argument on the case in February. (We've reported on that case here and here.) The central issue in the litigation is whether the SCA authorizes a court to direct providers to produce data stored overseas. The new CLOUD Act requires companies to provide information requested pursuant to the SCA "regardless of whether such communication, record or other information is located within or outside of the United States." But the CLOUD Act recognizes that comity concerns might justify resistance to such disclosure in the case of a foreign national. The Act authorizes the U.S. government to enter into agreements with foreign nations, enabling law enforcement in one country to obtain electronic data from providers in the other. The new statute provides that (only) when such agreement is in place and the U.S. government seeks to obtain from a provider data of a non-U.S. person residing abroad, that provider may move to quash on the grounds that compliance would materially risk violation of the "qualifying foreign government" who is party to that agreement. In addition, the CLOUD Act holds out the possibility that the SCA subpoena could be quashed even when there is no bilateral agreement or the target is a U.S. citizen or resident because it recognizes "common law standards governing the availability or application of comity analysis." As a ready measure of how much the new statute leaves open, the Microsoft case lives on. Microsoft and the government have advised the Supreme Court that they believe the CLOUD Act moots the current case. But the government has served a new order under that SCA (as now amended), and Microsoft is reportedly mulling a challenge on comity grounds; namely, that the data sought belongs to a citizen of Ireland and that country's law might prohibit Microsoft from complying.

Blood Doesn't Pay

And then there were 53. The U.S. Attorney's Office for the District of New Jersey announced that a New Jersey doctor was sentenced to 18 months in prison for his role in a test-referral bribe scheme operated by Biodiagnostic Laboratory Services LLC (BLS). Basel Batarseh, an internal medicine doctor with a practice in New Jersey, accepted bribes totaling more than $104,000 from BLS employees and associates between November 2007 and August 2010. In exchange, Batarseh generated more than $1.3 million in business for BLS. Batarseh is the 38th doctor and 53rd person overall to be convicted in this scheme. His sentencing, more than seven years after he accepted the last bribe, demonstrates that there may be more convictions to come.

False Claims Act and Corporate Integrity Agreements, Together for Now

Medical Transport, a Virginia-based ambulance service provider, agreed to pay $9 million to resolve allegations that it submitted false claims for ambulance transports in violation of the False Claims Act. Specifically, the government alleged that Medical Transport submitted false or fraudulent claims to Medicare, Medicaid and TRICARE for medically unnecessary ambulance rides and improperly billed rides to federal healthcare programs when they should have been billed to other payers. Notably, the settlement included a five-year corporate integrity agreement (CIA) with the U.S. Department of Health and Human Services Office of Inspector General (HHS-OIG). The CIA allows the government to monitor the activities of Medical Transport to ensure its compliance with the statutes, regulations, program requirements and written directives of Medicare and all other federal healthcare programs. For the press release, click here.

Medicare Fraud Strike Force Strikes Detroit Doctor

As explained here, an investigation stemming from the Medicare Fraud Strike Force resulted in a six-year prison term for a Detroit doctor for his role in a $10.4 million healthcare fraud scheme. After a one-week trial in September 2017, Mahmoud Rahim was convicted of one count of conspiracy to commit healthcare fraud and wire fraud, one count of wire fraud, one count of conspiracy to receive healthcare kickbacks, and two counts of receiving healthcare kickbacks. Evidence at the trial established that Rahim accepted kickbacks in exchange for referring Medicare patients for electromyogram tests (EMGs), some of which were unnecessary. Rahim identified these payments as "rent" and used a shell company to disguise his illegal activities. The district judge ordered Rahim to forfeit $1,679,505, along with restitution to be determined at a later date.

Deliberate Ignorance Instruction

The defendant in *Okechuku v. United States* filed a petition for certiorari with the U.S. Supreme Court. At issue is the level of review on appeal when a district court erroneously gives an instruction "allowing the jury to find a crime's required scienter through 'deliberate ignorance'—that the defendant purposely contrived to avoid learning that his conduct was criminal." Petitioner alleges a three-way split among the circuits that confront this argument on appeal: Two circuits hold that such an erroneous instruction is harmless per se, six hold it is harmless if there is "'sufficient' or 'substantial' evidence that the defendant had actual knowledge of criminal activity," and four "hold that it is harmless only if there is 'overwhelming' evidence of actual knowledge." As a result, the question presented is "[w]hether, and under what circumstances, the erroneous submission of a deliberate-ignorance instruction is harmless error." The response to the petition is due in mid-April, and the Court will decide whether to take the case in the coming months. To read the petition, click 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