january/february 2021

White Collar Roundup - January/February Edition

Defendants Miss Buzzer Beater in Bid to Overturn Fraud Convictions

The Second Circuit recently affirmed the fraud convictions of several defendants accused of paying tens of thousands of dollars to the families of top-tier high school basketball recruits. *United States v. Gatto*, 986 F.3d 104 (2d. Cir. 2021). Among other things, the court rejected the claim that the fraud convictions were invalid in light of the Supreme Court's decision in the Bridgegate case, a topic covered here in a prior White Collar Roundup.

The defendants in the case included Adidas' director of global sports marketing for basketball, an Adidas consultant, and an aspiring sports agent. Each was charged with wire fraud and conspiracy to commit wire fraud for their role in paying the families of top recruits—some of whom eventually went on to play in the NBA—to convince the players to attend Adidas-sponsored universities. The government alleged the defendants defrauded the universities by causing the recruits to falsely certify they were eligible for athletic-based aid. If the universities had known the recruits had accepted money and were ineligible to play, the aid could have gone to other athletes.

Following trial, the defendants were convicted and sentenced to terms of imprisonment ranging from six to nine months. One of the key arguments on appeal was that the universities' athletic-based aid was not an "object" of the defendant's scheme, as required by the wire fraud statute. On the contrary, the defendants claimed their intent was to *help* the universities by bringing in top recruits, which would improve performance and sponsorship revenues. The defendants claimed this argument was buoyed by *Kelly v. United States*—the Bridgegate case—where the Supreme Court reaffirmed that so-called "property fraud" convictions cannot stand if the property was merely "incidental" to the overall scheme. 140 S.Ct. 1565 (2020).

The Second Circuit disagreed, rejecting the analogy between the payments to college basketball recruits and the ill-fated traffic jam in Bridgegate. Writing for the majority, Judge Denny Chin concluded that the loss of property—the athletic-based aid from the universities—was at the "heart" of the defendant's scheme. If the universities had not awarded the aid, the recruits would have gone elsewhere. The court proceeded to deny the defendants' remaining arguments and affirmed their convictions in a divided opinion. Writing in dissent, Judge Gerald Lynch found that the District Court had erred in excluding from the trial evidence of phone calls between the defendants and college basketball coaches, and would have vacated some, but not all, of the convictions.

The outcome in *Gatto* suggests that the Supreme Court's decision in *Kelly* is not a one-size-fits-all defense to federal fraud convictions. The facts in the Bridgegate case were, to say the least, unusual. As a result, when defendants claim their own fraud convictions are invalid in light of *Kelly*, the courts may cry foul.

End of the (Fishing) Line—Grand Jury Lands Trump Tax Records

Back in the summer of 2020, we discussed the then-pending litigation stemming from New York County District Attorney Cyrus Vance's efforts to obtain then-President Trump's tax records on behalf of a grand jury. In the article, we commented on U.S. District Judge Victor Marrero's careful decision examining the so-called "fishing expedition" objection to grand jury subpoenas, in which he filleted the argument. *Trump v. Vance*, No. 19 CIV. 8694 (VM), 2020 WL 4861980 (S.D.N.Y. Aug. 20, 2020).

Later in the fall, we followed the case up to the Second Circuit Court of Appeals. There, the Second Circuit tossed the fishing expedition argument overboard, and affirmed the District Court's decision. *Trump v. Vance*, 977 F.3d 198, 205 (2d Cir. 2020). However, the district attorney agreed in advance that, in the event of an affirmance, he would not seek enforcement of the grand jury's subpoena if there were an appeal to the U.S. Supreme Court. Indeed there was, and though brought as an "emergency" appeal, the matter remained anchored without resolution throughout the fall and into the early winter of 2021.

Unusually, the Supreme Court did not then act upon the appeal, and it remained pending until late this February when, in a succinct order, the Supreme Court declined to hear the case: "The application for a stay presented to Justice Breyer and referred to the Court is denied." Thus, the fishing trip appears to have ended, and as we write this, the district attorney's office has announced they have received from Trump's accounting firm and are reviewing the tax and other records sought by the New York County grand jury. Former President Trump, however, did not abandon the maritime metaphor, arguing that the Supreme Court "never should have let this 'fishing expedition' happen, but they did."

So where does this leave prosecutors and defense counsel? Thanks to Judge Marrero and the Second Circuit, both now have a detailed and exhaustive set of opinions outlining the scope of grand jury subpoenas. But perhaps in one sense, little has actually changed. Cries of "fishing expedition" are likely to remain among the final, though usually floundering, efforts of other defendants to resist a grand jury subpoena.

New AMLA Aims to Hang Dirty Laundry Out to Dry

When Congress overrode the veto of former President Trump and passed the National Defense Authorization Act (NDAA) in January, it took a stand against something else as well: international money laundering. Within the sprawling NDAA, Congress passed the Anti-Money Laundering Act of 2020 (AMLA), which constitutes a major update to the anti-money laundering regulations of the Bank Secrecy Act of 1970 (BSA) and the financial terrorism apparatus of the USA PATRIOT Act of 2001. The AMLA's purpose is to modernize federal, state, and local law enforcement approaches to money laundering by granting regulators broader authority and resources and by simultaneously heightening reporting requirements on financial institutions.

The AMLA, for example, expands the authority of the DOJ and the Financial Crimes Enforcement Network (FinCEN) within the Treasury Department to respond to the modern challenges of deterring money laundering on a global scale. Under the Act, for example, the DOJ now has the authority to subpoena *any* account at a foreign bank that maintains a correspondent account in the United States, so long as the records are relevant to an ongoing investigation. FinCEN now has the authority to promulgate its own BSA-related regulations and work directly with the private sector to increase its monitoring capability. With greater authority, however, comes increased oversight. The DOJ must submit an annual report to Congress explaining any non-prosecution agreements entered into with financial institutions. Treasury, among other things, must conduct a year-long review of existing BSA regulations.

The AMLA also seeks to modernize. It amends the BSA's definition of financial institution to include entities that deal in currency substitutions, or cryptocurrencies. It mandates that Treasury establish a Subcommittee on Innovation and Technology and appoint an innovation officer in FinCEN to support law enforcement agencies with new technologies to aid in BSA compliance.

The AMLA further expands whistleblower protections and incentives, bringing these standards in line with similar Securities and Exchange Commission whistleblower regulations. For example, whistleblowers who provide voluntary information that leads to the recovery of more than $1 million may receive an award of up to 30% of the assets collected. They are also given greater relief should they prevail in a retaliation complaint against their employer.

The AMLA also requires certain qualifying corporations to provide information identifying their beneficial owners to FinCEN, who will maintain a database called the Beneficial Ownership Registry. Though the number of qualifying corporations is limited (it does not include publicly traded companies or those that employ at least 20 people within the United States and file federal tax returns exceeding $5 million), the Registry will serve as a helpful tool for regulators to identify suspicious financial activity and for private sector businesses to conduct more thorough due diligence before applicable transactions.

While many of these developments may not fully be felt for a number of years, the passage of the AMLA certainly signifies Congress' heightened interest in regulating financial institutions and countering financial terrorism. And it bodes well for a resurgence of law enforcement efforts in the coming years aimed at hanging global money laundering out to dry.

The More Things Change, the More Schemes Stay the Same

The Department of Justice (DOJ) recently announced the arrest of a 24-year-old cryptocurrency trader for allegedly making false representations in furtherance of an elaborate crypto-fund Ponzi scheme. Jeremy Spence, also operating under the name "Coin Signals," allegedly lured investors to his funds by touting returns of up to 148%. Spence succeeded in attracting

over $5 million in the form of Bitcoin and Ethereum from more than 170 different investors. Rather than generate enormous returns, however, Spence's crypto funds consistently lost money and ultimately left his investors $5 million poorer.

Spence was charged with one count of commodities fraud and one count of wire fraud, and faces up to 30 years in prison. His troubles mounted when the Commodity Futures Trading Commission (CFTC) also announced a federal civil enforcement action against him in connection with the same scheme.

While the environment of the cryptocurrency markets may have been newer, the rest of the fraud shared many of the hallmarks of a traditional Ponzi scheme. According to the FBI assistant director-in-charge, Spence had to use money obtained from new investors to pay off other investors because his trades were significantly less successful than he represented. Spence ended up distributing cryptocurrency worth approximately $2 million to his investors, but substantially from funds previously deposited by other investors.

The DOJ release provides good advice to investors in the crypto markets, urging education in "cryptocurrency ecosystems" which, just like more traditional markets, are subject to investment scams and fraudulent schemes. Whether in the cryptocurrency markets or otherwise, one thing remains the same: investors would do well to be wary of fund managers claiming enormous returns, and especially those presenting themselves as 24-year-old wunderkinds.

DOJ Continues to Hack Away at Cybercrime

In late February, the DOJ unsealed an indictment in the Central District of California in an escalation of its fight against cyber attacks by operatives sanctioned by the North Korean government. The indictment expands on the criminal complaint filed against one of the cyber operatives, Park Jin Hyok, in 2018. The DOJ's recent release accompanying the new indictment can be found here, and the release from the 2018 charges here.

The new indictment charges three members of North Korea's Reconnaissance General Bureau, a military intelligence agency, with conspiracy to perpetuate cyberattacks. The three individuals charged were alleged to be stationed in various countries, including China and Russia, as they worked to perpetuate crimes against the United States and other countries.

The indictment describes diverse and creative cyberattacks against numerous institutions. The North Korean operatives allegedly attacked companies with ransomware, and conspired to steal over $1.3 billion from foreign and domestic banks. And, perhaps most famously, the operatives breached Sony Pictures Entertainment in retaliation for the comedy film *The Interview*. The indictment also outlines how the operatives created malicious cryptocurrency applications, fraudulently marketed a block chain platform, and waged many spear phishing attacks against the U.S. Departments of State and Defense.

The indictment tells a truly chilling story of a global cybercrime campaign and the pervasiveness and creativity with which attackers infiltrated the digital realm in the United States and abroad. It serves as a stark reminder that warfare is becoming virtual, and foreign military units can work from anywhere to bring corporations or industries to their knees. At the same time, the high-profile indictment demonstrates an increasing ability and sophistication of the DOJ to pursue cyber wrongdoers wherever they may be found. And found, and brought to justice, we hope they may be.

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