SPEECHES & TESTIMONY

Speech of Enforcement Director James M. McDonald Regarding Enforcement trends at the CFTC, NYU School of Law: Program on Corporate Compliance & Enforcement

November 14, 2018

As Prepared for Delivery

Introduction

Thank you for that introduction. I'm happy to be back here at NYU as part of the Program on Corporate Compliance & Enforcement (PCCE). Over the years, the PCCE has brought together some of the best thinking in the enforcement, business, and academic community to develop a richer and deeper understanding of the causes of corporate misconduct, and how enforcement and compliance programs can most effectively deter it. The result is that the work here at the PCCE has been a driver of some of the most significant developments in Enforcement and Compliance.

We've followed these developments closely at the Commodity Futures Trading Commission (CFTC). At every stage of our agency's history, we've sought to bring impactful enforcement actions in the markets we regulate, and to ensure we stand ready to meet the challenges presented as these markets continue to evolve. Our most recent challenges have included responding to the dramatic expansion of our jurisdiction under Dodd-Frank in the wake of the financial crisis. Under David Meister, the first post-Dodd-Frank Director of Enforcement, the Division literally wrote the rules that set out some of our new enforcement jurisdiction. With the next Director, Aitan Goelman, the Division brought first-of-their-kind cases under these new rules. And under both Directors' leadership, we began to define our major priorities and to develop some of the initiatives we rely on today, like the Division's cooperation program. Thanks to their hard work and that of the dedicated career civil servants who staff the Division, we're well positioned today to continue to build on those priorities and initiatives. As part of that effort, we're constantly surveying the enforcement world to identify best practices and to incorporate them into our program.

The work of the PCCE has been particularly helpful to us in this regard. In fact, it was only a little more than a year ago that we talked about some of our priorities here at the PCCE. We emphasized in particular the development of the Division's cooperation and self-reporting program.

But a lot has happened at the CFTC in the past year. So my plan tonight is to do three things. First, to give you an update on what we in the Division have been up to over the last year. Our most recent Fiscal Year closed on September 30. This evening, in connection with this speech, we're releasing the Division's first Annual Report, which details our work during the last Fiscal Year. To save you the suspense, the report shows that, by any measure, enforcement during the past Fiscal Year has been among the most vigorous in the history of the CFTC.

Second, I'll outline some of the major priorities and initiatives that guided us over the last Fiscal Year and that will continue to guide us going forward. And finally, I'll offer an update on some recent developments in our cooperation and self-reporting program.

FY 2018 Overview

I'll start with an overview of our last Fiscal Year. But before I begin, let me say a word about how we measure our success. Any time we talk about year-end results, some of that discussion necessarily includes numbers. But a strong enforcement program is about more than just numbers. It's about preserving market integrity, protecting customers, and deterring potential bad actors from engaging in misconduct in the first place. It's about being tough, to be sure, but it's also about being fair. And it's about allocating resources efficiently to ensure our efforts target the most pernicious forms of misconduct. These sorts of things can't be measured by numbers alone. But that's a good thing: Federal agencies should not be motivated to hit certain numbers when enforcing the law.

At the same time, we recognize that numbers do tell part of the story. They might help show the direction an enforcement program is heading. They might reflect the types of cases that stand as priorities. Or they might offer some perspective on the program's broader goals. So in our annual report—and this evening—we offer quantitative and qualitative measures to tell the full story of our enforcement program.

The Annual Report walks you through these numbers, so I won't belabor them here. But I'll share with you the headline: This was a year of incredibly vigorous enforcement at the CFTC. That's true whether you measure it by the number of filed cases (third highest in CFTC history), amount of penalties imposed (fourth highest), number of large-scale matters (highest), types of cases charged (most ever involving manipulative conduct), number of parallel criminal actions (highest), percentage of cases that include individual charges (more than 2/3), or the number and amount of whistleblower awards (highest on both counts). For more detail on these numbers, I refer you to the Annual Report.

FY 2018 Priorities and Initiatives

What I'd like to do for the rest of the evening is to take you behind these numbers—to walk you through how these numbers reflect our priorities, and how we've begun or continued initiatives to advance these priorities.

Let's start with priorities. Our enforcement program over the last year largely centered around four priorities: (1) preserving market integrity; (2) protecting customers; (3) promoting individual accountability; and (4) enhancing coordination with other regulators and criminal authorities. Let me say a few words about each.

Preserving market integrity. Well-functioning commodity and derivatives markets are necessary to ensure the stability in prices that customers have come to expect, and the growth in the economy that Americans enjoy. When these markets are working, producers are able to hedge the risk that this year's output might not be as good as the last, which protects them and consumers against price increases. And these markets allow entities and individuals to allocate their capital more efficiently, which contributes to the growth of the broader American economy. But these markets won't function well if participants don't have confidence in the integrity of the market. That is why the Division has focused on detecting, investigating, and prosecuting misconduct that has the potential to undermine market integrity—misconduct like manipulation, spoofing, and disruptive trading.

These cases are complex, and they can be difficult. But they're essential. A primary function of our markets is to facilitate the price discovery process. And one of our principal responsibilities as regulator of these markets is to ensure that the price discovery process is sound. That means identifying, investigating, and prosecuting those who seek to interfere with this price discovery process.

The work of the Division over the last Fiscal Year reflects this priority. During Fiscal Year 2018, we brought more cases involving this type of misconduct than ever before. Indeed, from 2009 to 2017, the CFTC, on average, brought about six such cases per year. This past year, we filed twenty-six.

Many of these cases required us to address particularly complex and novel patterns of manipulation—including those that cross markets, cross exchanges, or even cross international borders.[1] Others required us to adapt to relatively new forms of manipulative conduct—like those that abuse technology or seek to manipulate the structure of the electronic order book.[2]

Protecting customers. Since its inception, the CFTC has focused on protecting customers in its markets from fraud and other forms of abuse. That focus remained a priority during the last Fiscal Year. The Division aggressively prosecuted fraud in some of these traditional areas, like precious metals, forex, and binary options. But this last Fiscal Year, we also saw some fraudsters evolve, as they sought to use new products or new technologies to target unwitting customers in markets like virtual currencies. We have worked hard to ensure that we are evolving with these bad actors—and indeed, staying one step ahead.

We saw success in this area as well. In one of the largest binary options frauds ever brought by the CFTC, we charged a massive national and international binary options fraud ring, which we allege harmed approximately 75,000 victims.[3] We charged numerous cases involving fraud in connection with virtual currencies.[4] We charged one case that started out as a binary options fraud and then morphed into a virtual currency fraud during the life of the scheme.[5] And we have taken these cases to trial when necessary, winning significant trial victories during the past Fiscal Year—including a precedent-setting victory in a trial involving Bitcoin fraud.[6]

Promoting individual accountability. A consensus has now developed in the enforcement and business communities that individual accountability must sit at the center of any effective effort to deter misconduct. We share in that consensus. It's not enough simply to hold the responsible companies accountable. The responsible individuals must be held accountable too. Individual accountability ensures that the person committing the illegal act is held responsible and punished; it deters others, fearful of facing individual punishment, from breaking the law in the future; it incentivizes companies to develop cultures of compliance and to report to regulators when they find bad actors in their entity; and it promotes the public's confidence that we are achieving justice. In pursuing individual accountability, we must look beyond the employees who actually commit the wrongful acts. We must also seek to hold accountable the supervisors and others in control who may be culpable as well.

We prioritized individual accountability during the past Fiscal Year, with more than two-thirds of our cases involving charges against individuals. We've charged individuals at financial institutions,[7] proprietary trading firms,[8] and managed funds.[9] We've charged primary wrongdoers, and also those who have facilitated that misconduct as aiders and abettors.[10] And we've used all available theories of liability that allow us to reach up the chain, like supervisory and control person liability—leading to charges against supervisors and desk heads,[11] CEOs,[12] and a Chairman of the Board.[13]

Enhancing coordination with other regulators and criminal authorities. We can most effectively protect our markets when working closely with our colleagues in the enforcement and regulatory community, both domestic and international. That is particularly true as our markets evolve and become more interconnected. Bad actors, it turns out, don't conform their misconduct to the technical boundaries of different regulatory jurisdictions, nor do they pause as their conduct crosses international borders. So regulators here in the United States and abroad must work together to ensure the entire scope of the misconduct is identified, investigated, and prosecuted. This approach yielded results this past year, as we investigated and filed a numerous of actions in parallel with our enforcement and regulatory counterparts.

Particularly noteworthy is our expanded effort to charge cases in parallel with our criminal law enforcement counterparts. A robust combination of criminal and regulatory enforcement in our markets is critical to achieving optimal deterrence. Perhaps the most significant development on this front was the announcement of the parallel actions involving spoofing and manipulative conduct we filed together with the Department of Justice and Federal Bureau of Investigation in January 2018.[14] A senior member of the Justice Department stated that these filings constituted "the largest futures market criminal enforcement action in Department history."[15] These filings were equally significant for the CFTC, which filed charges against three financial institutions and six individuals for manipulative conduct and spoofing, including the largest civil monetary penalty ever imposed for spoofing-related misconduct.[16]

But during the last year we filed a number of other actions in parallel with our criminal counterparts as well. These include cases ranging from retail and virtual currency fraud, to manipulation of global benchmarks, to efforts to obstruct our investigation.[17] And that's just to name a few. All of this means that wrongdoers in our markets now face the reality not just of substantial fines, but also, in appropriate cases, the prospect of criminal prosecution. This marks a trend that we expect to continue going forward and, we believe, will significantly deter wrongdoers from committing misconduct in our markets.

So those are the priorities. How have we advanced them? By beginning or continuing several key initiatives during the past Fiscal Year. I want to talk about a few of these initiatives this evening.

Data analytics. Anyone in our markets knows that these markets are going through a revolution—a revolution from analog to digital, from pit trading to electronic order books, from human trading to algorithmic, and from stand-alone trading centers to interconnected trading webs. Emerging digital technologies are impacting trading markets and the entire financial landscape with far ranging implications for capital formation and risk transfer.

We've worked hard to keep pace with this technological change, and to ensure we stand at the cutting edge of the data analytics world. We've done this primarily in three ways: (1) increasing the amount of data available to the Division; (2) ensuring the Division has the tools necessary to assess, evaluate, and analyze the data; and (3) developing the human capital in the Division so we can marshal this data to uncover and prosecute illegal conduct in our markets.

Particularly significant in this area has been the realignment within the Commission to move the Market Surveillance Unit from the Division of Market Oversight into the Division of Enforcement. Our Market Surveillance Unit includes market experts, economists, statisticians, and quantitative analysts, among others, who are dedicated to detecting fraud, manipulation, and disruptive trade practices. They typically do this by analyzing available data—including the activities of large traders, key price relationships, and relevant supply and demand factors—and by building data analytical tools that can be used to detect misconduct across our markets. Integrating the Market Surveillance Unit into the Division of Enforcement reflects the data-centric approach we pursued during the last Fiscal Year, and expect to continue going forward.

Specialized task forces. Also during the last Fiscal Year, we expanded the foundation of our enforcement program into new areas where we see or suspect misconduct—areas like spoofing, virtual currency, and insider trading. Developing our program in these new areas presented a challenge: How do we move as quickly as required, while ensuring each of our teams, across each of our offices, approach the matters in a smart and consistent manner? Our answer was to develop a set of specialized task forces in the Division to ensure consistency, identify best practices, and develop new approaches and ideas based on past lessons learned. Each task force includes members from each of our offices, in Chicago, Kansas City, New York, and Washington, D.C. These task forces focus on four different substantive areas.

- **Spoofing and Manipulative Trading:** A little more than a decade ago, our markets moved from in-person trading in the pit, to computer-based trading in an electronic order book. The advent of the electronic order book brought with it significant benefits to our markets—it increased

information available, reduced friction in trading, and significantly enhanced the price discovery process. But at the same time, this technological development has presented new opportunities for bad actors. Just as the electronic order book increases information available to traders, it creates the possibility that false information injected into the order book could trick them into trading to benefit a bad actor.

Efforts to manipulate the electronic order book—which can include spoofing—are particularly pernicious examples of bad actors seeking to gain an unlawful advantage through the abuse of technology. These efforts to manipulate the order book, if left unchecked, drive traders away from our markets, reducing the liquidity needed for these markets to flourish. And this misconduct harms businesses, large and small, that use our markets to hedge their risks in order to provide the stable prices that all Americans enjoy. The Spoofing Task Force works to preserve the integrity of these markets.

- **Virtual Currency:** The story of virtual currency is also about new technology. And it is a story about the need for robust enforcement to ensure technological development isn't undermined by the few who might seek to capitalize on this development for unlawful gain. New and potentially market-enhancing technologies like virtual currencies and distributed ledger technology need breathing space to survive. Through work across the Agency, the CFTC has shown its continued commitment to facilitating market-enhancing innovation in the financial technology space. But part of that commitment includes acting aggressively to root out fraud and manipulation from these markets. The Virtual Currency Task Force is dedicated to identifying

misconduct in these areas and holding bad actors accountable.

- **Insider Trading and Protection of Confidential Information:** Illegal use of confidential information can significantly undermine market integrity and harm customers in our markets. This type of misconduct could include misappropriating confidential information, disclosing a client's trading information, front running, or using confidential information to unlawfully prearrange trades. As we continue to build the foundation of our enforcement program, we will continue to work to ensure our market participants are not misappropriating confidential information for their own benefit.

- **Bank Secrecy Act:** Many of our registrants are required to comply with the Bank Secrecy Act and anti-money laundering rules. These registrants' obligations include following rules related to suspicious activity reporting (SAR) and know-your customer programs (KYC). These laws exist for good reason, as they require these market participants that serve as a first-line of defense against fraud, money-laundering, and related offenses to be on the lookout for misconduct. Indeed, SARs and other Bank Secrecy Act reports significantly contribute to the Division's ability to detect and prosecute the sort of misconduct that may flow through our registrant intermediaries. Our Bank Secrecy Act task force works to ensure all of our registrants live up to these obligations.

Cooperation and Self-Reporting: Recent Developments

The final item I'll discuss this evening is our cooperation and self-reporting program. Last year, we explained our view that this program would serve as a powerful tool to hold wrongdoers in our markets accountable. We explained that the program is designed to get companies and individuals who know about the misconduct to tell us about it; to enable us to identify all of those involved in the wrongdoing; and to allow us to prosecute the most culpable individuals and companies. It's a tool that originated in organized crime and gang prosecutions, and has been employed aggressively and with success in white collar prosecutions as well. We've now incorporated this tool into our enforcement efforts at the CFTC.

We're still just getting started, but the early returns look good. Through the end of last Fiscal Year, we had issued three significant orders that involved self-reporting. Each included a civil monetary penalty that reflected a significant reduction on account of the self-report, cooperation, and remediation.[18] We also employed our individual cooperation program to sign up individuals to cooperation agreements, which also led to significantly reduced penalties—some of which even included no civil monetary penalty.[19]

When we announced the program, we made clear that it should not be viewed as giving anyone a pass. That's been borne out over the last year, in which we filed cases against more financial institutions than any prior year but one. We brought charges against several individuals who work at these institutions. And through our cooperation and self-reporting program, we were able to charge both companies and individuals, including supervisors and senior management, that we otherwise might not have been able to charge.

What's more, this program is continuing to grow. We're only a little more than five weeks into the new fiscal year. Yet already we've had two significant new developments.

The first involved spoofing and manipulation charges against Kamaldeep Gandhi, formerly a trader at several proprietary trading firms. As part of our investigation, Gandhi agreed to cooperate with the CFTC and entered into a cooperation agreement with the Division. Under the terms of that agreement, Gandhi admitted to his own conduct, and told the CFTC about others who were also involved. Among other things, Gandhi's cooperation agreement binds him to continue to cooperate throughout the course of the CFTC's broader investigation.

Because Gandhi's cooperation was not yet complete at the time of the resolution, the CFTC bifurcated Gandhi's case—deciding liability in an order issued on October 11, 2018,[20] but leaving the amount of the penalty to be determined at a later date, once Gandhi's cooperation is complete. This bifurcation mirrors the criminal process, where the guilty plea comes first, and sentencing later. And bifurcation allows the CFTC to consider the entire range of cooperation when determining the appropriate penalty. Gandhi's case stands as an example of the sorts of tools we'll employ to ensure we can use our cooperation program in the most effective way possible. I expect you'll see more bifurcated orders in these types of cases going forward.

The second development involved a case announced last week involving a former managing director at Deutsche Bank named Jacob Bourne. During June and July of 2017, Bourne mismarked the valuations of swaps in an attempt to cover up more than $10 million in trading losses. The mismarked swaps were then reported to counterparties and the CFTC.

Deutsche Bank's internal controls identified the discrepancies in Bourne's swap valuations. Having caught the discrepancies, the bank conducted an internal investigation, which determined that Bourne had mismarked the swaps in question and then altered documents to cover it all up. The bank moved quickly to reach this conclusion: The bank identified the discrepancies less than a week after Bourne began mismarking the swaps, and it reached its conclusion less than a month later. Three days after that, the bank self-reported Bourne's conduct to the Division. Bourne was placed on administrative leave and then terminated.

The CFTC brought an action against Bourne for fraud arising out of this mismarking. But the Division declined to prosecute the bank, on account of its self-reporting, cooperation, and remediation. The declination letter is available on the CFTC's website, and it includes more detail, which I recommend you read.

But stepping back just a bit, the takeaway here is that this is how our self-reporting program is designed to work. We want companies to have sufficient internal controls to catch wrongdoing when it happens. When they find misconduct, we want them to take appropriate remedial steps—to fix the problem, and to make sure it won't happen again. And yes, we also want them to tell us about it, and to cooperate proactively in our investigation. If they do that, the individuals responsible will be prosecuted, as Bourne was here. But the company will gain a substantial benefit as a result of their self-report, cooperation, and remediation. And in extraordinary cases like Deutsche Bank's, the company may receive a declination of prosecution altogether.

Stepping back even further, this all really goes to the heart of what we're trying to achieve with our enforcement program more generally. The end goal for us in Enforcement extends well beyond the number of cases filed, or the amount of penalties imposed. We intend for our enhanced emphasis on individual accountability, cooperation, and self-reporting—together with the other priorities I've discussed this evening—to have a far broader social impact. Our end goal is to foster a true culture of compliance in our markets.

What do we mean when we talk about a culture of compliance? Think about it this way: Imagine a CEO standing in front of the company's new hires on their first day on the job. Imagine the CEO telling the new staff about the various trainings to come as part of the onboarding process—compliance, ethics, human resources and the like. And imagine the CEO telling the new staff that, notwithstanding these various internal company regimes, if they break the law, their problems won't stop with the compliance, ethics, or human resources department. Their problems will come from the CFTC (and perhaps even the DOJ and the FBI). That's because, the CEO tells the staff, the company is committed to identifying any misconduct, and to reporting it out to the relevant authorities.

That's the sort of commitment we're seeking to foster. That's the sort of commitment that creates the culture of compliance we want to see in all of our market participants. And that's the end goal to which all of our enforcement efforts are aimed.

We believe this past Fiscal Year, particularly when viewed in light of the robust enforcement program we've built over the years, shows that we've taken significant steps towards achieving this culture of compliance in our markets. We'll work hard during this next Fiscal Year and beyond to ensure this trend continues.

Thank you.

[1] *See, e.g.*, *In re Victory Asset, Inc.*, CFTC No. 18-36, 2018 WL 4563040 (Sept. 19, 2018) (consent order); *In re Ramsey*, CFTC No. 18-49, 2018 WL 4772228 (Sept. 27, 2018) (consent order).
[2] *E.g.*, *CFTC v. Thakkar*, No. 18-CV-00619 (N.D. Ill. filed Jan. 28, 2018); *In re Geneva Trading USA, LLC.*, CFTC No. 18-37, 2018 WL 4628252 (Sept. 20, 2018) (consent order).
[3] *CFTC v. Atkinson*, No. 18-CV-23992 (S.D. Fl. filed Sept. 27, 2018); *CFTC v. Montano*, No. 18-CV-1607 (M.D. Fl. filed Sept. 27, 2018); *In re Berry*, CFTC No. 18-42, 2018 WL 4772227 (Sept. 27, 2018) (consent order); *In re Pollen*, CFTC No. 18-43, 2018 WL 4772232 (Sept. 27, 2018) (consent order); *In re Barrett*, CFTC No. 18-44, 2018 WL 4772230 (Sept. 27, 2018) (consent order); *In re Brookshire*, CFTC No. 18-45, 2018 WL 4772229 (Sept. 27, 2018) (consent order); *In re Schranz*, CFTC No. 18-46, 2018 WL 4772231 (Sept. 27, 2018) (consent order); *In re Giacca*, CFTC No. 18-47, 2018 WL 4772226 (Sept. 27, 2018) (consent order); *In re Stephenson*, CFTC No. 18-48, 2018 WL 4772233 (Sept. 27, 2018) (consent order).
[4] *CFTC v. McDonnell*, No. 18-CV-361, 2018 WL 4090784 (E.D.N.Y. Aug. 28, 2018).
[5] *CFTC v. Kantor*, No. 18-cv-02247-SJF-ARL (E.D.N.Y. filed Apr. 16, 2018).
[6] *See McDonnell*, 2018 WL 4090784; *see also CFTC v. Gramalegui*, No. 15-CV-02313, 2018 WL 4610953 (D. Colo. Sept. 26, 2018).
[7] *E.g.*, *CFTC v. Vorley*, No. 18-CV-00603 (N.D. Ill. filed Jan. 26, 2018).
[8] *E.g., CFTC v. Mohan*, No. 18-CV-00260 (S.D. Tex. filed Jan. 28, 2018).
[9] *In re Franko*, CFTC No. 18-35, 2018 WL 4563039 (Sept. 19, 2018) (consent order).
[10] *CFTC v. Thakkar*, No. 18-CV-00619 (N.D. Ill. filed Jan. 28, 2018).
[11] *See, e.g.*, *CFTC v. TFS ICAP, LLC*, No. 18-CV-8914 (S.D.N.Y. filed Sept. 28, 2018).
[12] *See, e.g.*, *id.*
[13] *In re Leibowitz*, CFTC No. 18-52, 2018 WL 4828377 (Sept. 28, 2018) (consent order).
[14] James M. McDonald, *Statement in Connection with Manipulation and Spoofing Filings* (Jan. 29, 2018) (*McDonald Statement*), https://www.cftc.gov/PressRoom/SpeechesTestimony/mcdonaldstatement012918.

[15] John P. Cronan, *Acting Assistant Attorney General John P. Cronan Announces Futures Markets Spoofing Takedown* (Jan. 29, 2018), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-john-p-cronan-announces-futures-markets-spoofing.
[16] *McDonald Statement*, *supra* note 14.
[17] *See, e.g.*, *CFTC v. Landgarten*, No. 18-CV-03824 (E.D.N.Y. filed July 2, 2018); *CFTC v. Kantor*, No. 18-cv-02247-SJF-ARL (E.D.N.Y. filed Apr. 16, 2018) (retail and virtual currency fraud); *In re Société Générale S.A.*, CFTC No. 18-14, 2018 WL 2761752 (June 4, 2018) (consent order) (benchmark manipulation).
[18] *In re The Bank of Nova Scotia*, CFTC No. 18-50, 2018 WL 4828376 (Sept. 28, 2018) (consent order); *In re UBS AG*, CFTC No. 18-07, 2018 WL 684636 (Jan. 29, 2018) (consent order); *In re The Bank of Tokyo-Mitsubishi UFJ, Ltd.*, CFTC No. 17-21, 2017 WL 3433489 (Aug. 7, 2017) (consent order).
[19] *See, e.g.*, *In re Brookshire*, CFTC No. 18-45, 2018 WL 4772229 (Sept. 27, 2018) (consent order).
[20] *In re Gandhi*, CFTC No. 19-01, 2018 WL 5084650 (Oct. 11, 2018) (consent order).