

## Options Clearing Corp.'s CRO for the SIFMU Era

Veteran financial risk manager John Fennell pursues a comprehensive, enterprise-wide mandate as the systemically important Chicago-based CCP's chief risk officer.

By Jeffrey Kutler

November 23, 2016

For a select few clearing and settlement institutions, Title VIII of the Dodd-Frank Act of 2010 introduced the notion of Systemically Important Financial Market Utilities, as designated by the U.S. Treasury-led [Financial Stability Oversight Council](#). "The Dodd-Frank and related FSOC provisions are designed to promote robust risk management and safety and soundness, reduce systemic risk, and support the stability of the broader financial system," Options Clearing Corp. explained when it announced its SIFMU designation in [July 2012](#). "OCC expected this designation, which reflects its critical role within the U.S. financial markets infrastructure."

That was but one stage of an ongoing managerial and cultural transformation for Chicago's OCC, which is the world's largest equity derivatives clearing organization and provides central counterparty (CCP) services to 19 exchanges and trading platforms for options, financial futures, security futures and securities lending transactions. The January 2014 arrival of former CME Group chief executive officer Craig Donohue as [executive chairman](#) accelerated those changes, with Donohue taking charge of control functions (enterprise risk management, internal audit and corporate compliance) and external affairs (government relations and corporate communications - Options Industry Council).

In September 2016, [OCC announced](#) that Donohue, now executive chairman and CEO, would be staying on for three more years. Among other personnel moves, executive vice president of financial risk management John Fennell was promoted to EVP and chief risk officer, replacing John Grace, who left the company.

"Thanks to our talented team, OCC is evolving from a clearing and settlement utility to becoming a systemically important market influencer, with increased emphasis on risk management and the resiliency required to effectively manage risk for the U.S. listed equity options and futures markets," Donohue stated, adding, "The OCC board of directors agrees that we have accomplished much and have the chance to do more . . . While we have made great strides, much more opportunity lies ahead for OCC."

For risk management, the leadership it entails and the robust culture that sustains it, Fennell is front and center. A DePaul University MBA who has completed the Certified Regulatory and Compliance Professional program of the FINRA Institute at the University of Pennsylvania's Wharton School, Fennell joined OCC in 1993, initially working in operations and technology. He has been in the risk management area for 17 years, and in his previous financial risk management post was responsible for market, credit and liquidity risk, default management, customer margin methodologies and model development.

As CRO, Fennell is responsible for implementing OCC's risk management strategy while also overseeing the model validation and enterprise risk management departments, security services, business continuity and disaster recovery, and vendor risk management.

"Risk is our business," Fennell asserts. "We think about it constantly and are constantly investing in it."

He says that "prior to 2012, the company operated well, but in a less formal way." He describes the SIFMU designation as "like a Sarbanes-Oxley for CCPs." That was an impetus, under Donohue, to introduce "not only the disciplines, risks and controls of a public company, but also the kind of risk culture that, at the end of the day, will drive how we behave and make the processes repeatable. That was a major shift for us."

CRO Fennell elaborated on the pre- to post-crisis evolution at OCC and in financial market infrastructures more broadly in this recent interview with GARP editor-in-chief Jeffrey Kutler.

### **How has OCC's risk management changed since the crisis?**

Prior to the financial crisis, clearing was regarded as a back-office function for settling trades, moving money, and risk-managing the transactions as part of that. The financial crisis, from my perspective, altered that thinking: Clearing is central and critical to the operations of financial markets, and a key component of that is risk management. Out of the financial crisis, risk management was elevated in the eyes of the regulators, and rightfully so. Other pieces of that are transparency, governance, the repeatability of those processes – an assurance that in a crisis or any kind of event, the functions of the CCP would be repeatable, and the markets would have an understanding of how the CCP would behave.

### **What differences did the SIFMU designation bring about?**

Prior to that, the risk organization was structured as a small group of generalists responsible for evaluating liquidity, credit, and market risks at a member level. But that structure made it challenging to (1) consider risks comprehensively across members, and (2) have a deep understanding of OCC's risks within these individual risk disciplines. One of the first things I focused on was to break out those different disciplines, so we could begin to develop a deep expertise in market, credit, liquidity risk as well as developing stress testing and default management departments. The intent was to create a level of expertise in these areas (default management, market risk, liquidity risk, etc.) and bring a comprehensive view of risk to the company so we could continue to evolve our capabilities from a risk perspective.

As CRO, I have moved into a new role, taking a more enterprise-wide view. It fits my capabilities well, given that I know the organization well, understand the risks of the organization very well, and now bring that knowledge and capability from a broader, enterprise-wide perspective. It's about bringing awareness of the company's risks to management so we can leverage that information to prioritize investments and incorporate risk management in the strategic decision-making process of the organization.



*"Clearing is central and critical to the operations of financial markets, and a key component of that is risk management," says OCC chief risk officer John Fennell.*

### **What is the role of the CRO in promoting an enhanced risk culture?**

Evolving the risk culture and its footprint is one of the things I am most excited about. Credibility is there, with peers and throughout the organization, because of my tenure and expertise. We can talk about clearing issues and share an understanding, whether it's technology, operations, finance and accounting – depth of knowledge is part of it. But what I'm really interested in doing is to ingrain the risk culture in the firm. That means, for example, having people look at their processes at a very granular level, people who are engaged in day-to-activities seeing issues first, and when they see something, say something. When people in an organization are not conditioned to escalate issues and bring awareness to them, those issues can continue to occur and become status quo. Our process is to identify and escalate issues right away and, with that awareness, figure out the best way to mitigate the risk. Our message is "identify, escalate, and then debate."

In the past, people might see a problem and try to fix it, but not bring awareness to it. That could lead to siloed solutions to issues that are only partially mitigated. Escalate the problem right away, and you can start addressing the risk in a more comprehensive way. That is a post-2012 evolution for us.

### **Did you draw on any "best practice" models?**

In a general sense, risk focus or risk culture has evolved over the last 10 years or so. Something we are going through now is a risk culture audit. We bring in a firm specifically to evaluate the culture, tone at the top, how we are communicating that message. A key component of infusing a risk culture in an organization is through compensation and performance evaluation. That can be very powerful, but it's tricky. If, for example, you set up a compensation structure that penalizes for too many internal audit findings, then that can create an incentive to not be transparent. You want to incent people to report and highlight issues. We are thinking about things like self-identified findings: In your internal audit review, what percentage of the findings are self-identified? The more of those that you have, the better an organization's risk culture. It shows that people are aware of the risks, are reporting the risks, and creating plans proactively to mitigate the risks. You have to be thoughtful and be sure you are incenting the right behaviors.

### **Whom do you report to?**

I report to the head of the risk committee of the board. Administratively, I report to the executive chairman and CEO, Craig Donohue. Likewise, the chief compliance officer and chief audit executive report solid-line to the board, and dotted-line administratively to Craig.

### **Is there a discrete risk management department that you oversee?**

My former role in financial risk management – handling credit, market and liquidity risk, etc. – is a first-line function, reporting to the chief administrative officer. Second-line risk functions – enterprise risk management, models validation and information security – report to the chief risk officer. The effective challenge and oversight aspects reside on the second line. Some CCPs do it differently, with all of the above reporting in to the CRO. Here, for example, we look at margin deposits, which, in theory, can be a competitive lever to attract volume and open interest. We separate that to provide an effective challenge on how we set margin levels – that is, volume versus prudent risk management.

### **Are more resources available for risk management?**

People-wise, in the core credit, market and liquidity risk functions, we have gone from a staff of 20 pre-crisis to 60 today. Pre-crisis, we didn't have an enterprise risk management department; today we have about 20 people in ERM. Compliance is a new department that has evolved since the crisis. So, from a people perspective, OCC has invested significantly in financial risk management, culture-wide risk management, compliance and model validation. Additionally, if you look at our IT investments, most of what we are and will be investing in is managing risks, incorporating models, processes to evaluate risks, and stress testing, which is a major area of investment over the last three to four years. As we go forward, we are looking to invest in getting more granular in risk assessment, getting more real-time – that is, looking at intraday risks from both a price and portfolio perspective for an understanding of how our risk profile changes during the day, rather than just looking at end-of-day closes.

We have also done a lot to address risks prior to the trades getting to OCC. We had a huge pre-trade risk controls initiative for evaluating whether trades are reasonably priced and identifying rogue algorithms. We are unique in that we clear for 19 different exchanges and trading platforms, in contrast to a vertical exchange model like CME or ICE where the clearinghouse serves just one exchange. So, from a third-party risk perspective, it is incumbent upon us to make sure that those who interface with us have good risk controls over how they evaluate a trade before introducing it to us for guarantee.

### **What technology is needed for intraday risk tracking?**

Everything starts with the core database, to make sure that you have your key risk components in place, that you are aggregating the data as it comes in. We really have to think about leveraging something close to high-frequency trading technology, and a more agile SDLC [systems development life cycle] type of development framework to be more nimble in how we design systems within a strong control environment. Our risks are evolving and changing quickly. When a new scenario like Brexit is emerging, it is key for us to have the flexibility to act by creating stress tests to know where the risks are proactively, rather than when the event is actually happening. Also, thinking about different database structures, different methods for processing transactions in computing our risk real-time and across all of the greeks, and then about how we design systems as efficiently as possible.

## **How big a concern is information security?**

It consumes a big part of my day. Given my financial risk background, technology and cyber risk is a new area for me and one that we will want to try to stay ahead in managing. If anybody wants to breach your walls, with enough resources and commitment to do it, they will. One has to, as quickly as possible, identify and quarantine the issue and then have continuity plans to mitigate the issue. In our world, we have access to federal-level resources as far as understanding when a potential cyber attack is emerging. Although we have built processes and have resources available to us, it's always about trying to improve the infrastructure, identify issues as they are emerging, and have robust contingency plans to react and mitigate the incident. Communications is important in all that – it may be a cyber event impacting us, or impacting one of our members – to be transparent and make people aware of the issue, and to ensure confidence. It is always No. 1 for a CCP to make sure that confidence is not eroding, that issues are addressed and mitigated and that business is continuing.

## **How do you keep an eye on technological innovations?**

In our governance, new technologies go through a risk vetting process before they are adopted. A good example now is the cloud. As we build up our risk analytics, and going from an overnight batch process to real-time process, data storage is going to be key, and it becomes imperative to access and leverage cloud technology. There are obvious risks involved: storing data on someone else's servers, making sure the data is secure – it is enterprise risk and information security. A key component of my role is to empower the firm for leveraging new technologies. But it has to be in a safe and secure way. We need to have a process to evaluate a new technology comprehensively to understand the risks, put mitigating controls in place and enable the business to take advantage of the technology. It's a different kind of risk if an organization is narrow-minded and takes years and years evaluating a technology and never gets to take advantage of it.

## **Do you engage directly with regulators?**

Our primary regulator is the Securities and Exchange Commission, but we also have the Federal Reserve and Commodity Futures Trading Commission as secondary regulators. They are looking to ensure that the firm has the proper governance to evaluate its risk proactively. There are regular touch points, whether I do it as part of the management committee, or independently as chief risk officer.

## **Do you get regulatory guidance on stress testing?**

The Principles for Financial Market Infrastructures (PFMI) have very high-level, principles-based guidance for CCPs. [CPMI-IOSCO](#) [Committee on Payments and Market Infrastructures and International Organization of Securities Commissions] recently came out with new guidance that is more prescriptive around the types of stress testing CCPs should do. While there is some direction out there on types of stress tests, whether for informational purposes or for sizing financial resources, my personal perspective is that what CCPs should be thinking about is based on their exposure. We all clear different and unique products in different environments. It is important that CCPs have comprehensive and robust processes for managing risks and establish stress tests that proactively identify aggregations of those risks. We internally have a stress testing committee that on a monthly basis evaluates the tests that we have and considers the environment for potentially new stress tests. Stress tests are core to what we do. I believe this is the intent of what the regulators are looking for with the new guidance.