OCC®: Planned Path to Cloud Adoption

OCC has filed an Advanced Notice with the Securities and Exchange Commission in connection with our proposed adoption of a "Cloud Infrastructure" hosted by a Cloud Service Provider ("CSP") to support OCC's new core clearing, risk management, and data management applications currently under development. Advance Notice Filings are required when systemically important financial market utilities ("SIFMU") propose actions that could have a material effect on the level or nature of risk presented by the SIFMU. Given OCC's critical role, we believe it is important to provide transparency to market participants about the filing and OCC's objectives.

The filing reflects our plan to use the virtual equivalent of physical data center resources via a "Virtual Private Cloud." The Virtual Private Cloud is the cloud-based equivalent of a traditional data center, and offers scalable resources that: (i) handle various computationally intensive applications with load-balancing and resource management ("Compute"); (ii) provide configurable storage ("Storage"); and (iii) host network resources and services ("Network"). Beyond the use of a multi-region cloud solution for primary and backup services, the proposal reflects OCC's plan to maintain an on-premises tertiary data center to provide the ability to support core clearing, risk management, and data management applications in the unlikely and extraordinary event of a multi-region outage of cloud-based Compute, Storage, and Network services impacting OCC operations at the CSP.

Today, OCC principally provides its core clearing, risk management, and data management service via ENCORE, which is run in two traditional, geographically diverse data centers located in Illinois and Texas. The ENCORE system was launched in 2000 and serves as OCC's processing engine receiving trade and post-trade data from a variety of sources on a transaction-by-transaction basis, maintaining clearing member positions, calculating margin and clearing fund requirements, and providing reporting to OCC staff, regulators, and clearing members.

ENCORE has accommodated industry growth in processing large volumes and OCC has managed periods of extreme market volatility and stress, including during the 2007-2008 financial crisis and the COVID-19 global pandemic of 2020-21, without interruption. Nevertheless, ENCORE was designed to operate in traditional on-premises data centers that require the acquisition and installation of additional hardware and systems software to accommodate heightened resource needs or new applications. In this regard, the resiliency and scalability of the current infrastructure is less flexible than that offered by Cloud Infrastructure.

OCC's proposed cloud implementation is a natural progression of our information technology strategy and aligns seamlessly with our overall corporate strategy, which is to:

- Reinforce OCC's foundational capabilities and deliver effective and efficient services;

- Deliver product and service enhancements that enable growth in OCC's core capabilities and provide capital efficiencies to market participants; and

- Demonstrate thought leadership in the delivery of innovative solutions that provide long-term value and efficiencies for OCC and its stakeholders.

OCC's objective is the replacement of ENCORE with a resilient solution that meets market participants' needs and the regulatory expectations for a SIFMU. Given advances in cloud technology and information security since 2000, OCC's proposed adoption of Cloud Infrastructure is an important component of achieving that objective.

Benefits of the Proposal

Cloud implementation will enable OCC to leverage the Compute, Storage, and Network capabilities of a

CSP, supplemented with compatible third-party vendor solutions, to maintain a modular architecture that will result in:

- Improved resiliency,

- Enhanced security, and

- Increased scalability for OCC's new core clearing, risk management, and data management applications.

Improved Resiliency

As a SIFMU, OCC must ensure that core applications have resiliency and recovery capabilities commensurate with OCC's importance to the functioning of the US financial markets. OCC believes cloud implementation will enhance the resiliency of OCC's core clearing, risk management, and data management applications by virtue of OCC's architectural design decisions, disciplined approach to deployment of Cloud Infrastructure, and the cloud's built-in redundancy and guarantee of persistent availability. As proposed, OCC would provision Compute, Storage, and Network resources in two autonomous and geographically diverse regions, in a hot (primary)/warm (back-up) configuration to increase resources available on demand, maintained by the CSP.

Each region consists of three zones, each of which has a physical infrastructure with separate and dedicated connections to utility power, standalone backup power sources, independent mechanical services, and independent network connectivity. While not dependent on one another, zones are connected to one another with private fiber-optic networking, enabling the infrastructure of core clearing, risk management, and data management applications to automatically failover between zones without interruption. Each zone can operate independently of one another and failover capability is near instantaneous i.e. a loss of one zone will not affect operations in another zone and no core clearing, risk management, or data management application will be reliant on the functioning of a single zone. This structural framework offers OCC a wide environment within which to run its core clearing, risk management, and data management applications while simultaneously restricting the effect of an adverse event at the CSP to the smallest footprint possible.

Each region will maintain independent and identical copies of all critical applications that are deployed by OCC, allowing OCC to transition its core clearing, risk management, and data management applications from one region to another seamlessly. Production workloads would be run across and shifted between regions regularly to protect OCC against disruptions from intra-regional incidents. In the unlikely event that a region is temporarily disabled as a result of an extreme event, OCC's applications would fail-over to run in the other region. At any point in time, OCC will have active primary and standby instances of the core clearing, risk management, and data management applications that can be moved to any of the six environments (i.e. three zones in each of the two regions). This is analogous to having six physical data centers with primary and backup systems running out of any two of them at a given point in time. OCC's proposed solution would significantly reduce operational complexity, mitigate the risk of human error, and provide resiliency and assured capacity. Additional capacity will be available to support the resiliency of OCC's core clearing, risk management, and data management applications by way of the six-way redundancy. Moreover, OCC will continue to periodically test the CSP's capacity scaling features and failover capabilities to ensure adequate capacity is available to OCC.

In addition to cloud deployment, OCC will maintain an on-premises data center to provide the ability to support core clearing, risk management, and data management services in the event of a multi-region outage at the CSP that impacts OCC operations. The on-premises data center will operate as a separate, logically isolated back-up to the six levels of redundancy provided for by the Cloud — a back-up to the back-ups — intended to be used only in the unlikely and extraordinary event that OCC completely loses access to the CSP. From an architectural perspective, the on-premises data center is similar to adding a third CSP region with a single zone. Most technologies will remain the same with a fail-over to the on-premises data center and core platform technologies that enable Compute, Network, and Storage services to be operated by OCC with synchronous data replication via dedicated, end-to-end encrypted links between the cloud and the on-premises data center and leaving member connectivity unchanged.

OCC believes cloud implementation will enhance the resiliency of OCC's core clearing, risk management, and data management applications by virtue of its built-in six levels of redundancy, which will provide OCC with easy access to multiple zones within multiple and geographically diverse regions. The redundancy provided to OCC in the Cloud Infrastructure helps ensure that Compute, Storage, and Network resources will be available to OCC on a persistent basis.

Enhanced Security

As a SIFMU and the exclusive provider of clearance and settlement services for listed options in the US, it is vital that OCC's critical services remain continuously available with sufficient security measures in place to detect and defend against possible security threats. The cloud implementation will present OCC with an agile operating environment that can scale throughput to match workloads nearly instantaneously and enable OCC to build a "secure by design" pervasive security methodology that incorporates the National Institute of Standards and Technology ("NIST") Cybersecurity Framework's functions as a roadmap for cloud security. Movement to an agile, cloud-based operating environment further reinforces OCC's commitment to building a comprehensive and adaptable risk-based security methodology instead of a traditional perimeter-centric model.

The physical and cyber security standards that OCC has designed to align with NIST, the Cyber Security Framework ("CSF"), and the Center for Internet Security ("CIS") benchmarks will not change in the proposed Cloud Infrastructure. OCC will add meaningful security capabilities and measures provided by the CSP and selected third-party tools to enhance the security of OCC's core clearing, risk management, and data management applications. Given the scope of their service, CSPs leverage economies of scale and offer infrastructure and services with specialized configuration, monitoring, prevention, detection, and response tools. Furthermore, unique cloud-specific capabilities, such as services for provisioning credentials and end-to-end configuration change management and scanning, will provide OCC enhanced levels of protection that is not available in traditional on-premises solutions. Finally, the back-up, on-premises data center will be physically isolated from other on-premises

networks, such as the development network, and will have consistent controls and equivalent security tools to that of the data centers accessed through the CSP.

OCC has established a robust cloud security program to manage the security of the core clearing, risk management, and data management applications that will be running in the cloud and to monitor the CSP's management of the security of the Cloud Infrastructure, which it operates. The enterprise security program encompasses all OCC assets in OCC offices, data centers, and within the Cloud Provider's Cloud Infrastructure. Identity and Access Management (IAM) controls will ensure "least privileged" user access to applications in the Cloud. OCC has appropriate controls in place to ensure the security of confidential information in-transit between OCC data centers and the Cloud Infrastructure, between systems within the Cloud Infrastructure, and at-rest. All network communications between OCC and the cloud will rely on industry standard encryption for traffic while in transit, and data at rest will be safeguarded through pervasive encryption. Finally, automated delivery of business and security capability via the use of the "Infrastructure as Code," cloud agnostic tools, and continuous integration/continuous deployment pipeline methods help to ensure security controls are consistently and transparently deployed.

Increased Scalability

The proposed cloud implementation will provide OCC with more dynamic scalability of Compute, Network, and Storage resources to support OCC's core clearing, risk management, and data management applications. In the current on-premises environment, immediate scalability is limited by the capacity of the on-premises hardware. Accordingly, OCC would need to obtain additional physical servers and network equipment to scale beyond the limits of the on-premises hardware, potentially affecting its ability to quickly adapt to evolving market conditions, including spikes in trading volume. In the cloud, however, additional Compute Storage, or Network resources can be launched on demand, so the scalability is considerable and instantaneous. With a Cloud Infrastructure, OCC can quickly provision or de-provision these resources to meet demands, including elevated trade volumes, increased creation of development and test environments for

back testing and stress testing, and other systems development needs.

Regulators' and market participants' expectations are for OCC to "be efficient and effective in meeting the requirements of its participants and the markets it serves," and to regularly review the "efficiency and effectiveness of our clearing and settlement operations and operating structure, including risk management policies, procedures, and systems." Consistent with these expectations, there are several significant efficiency benefits to the cloud implementation, including:

- Ad-hoc reporting capability with new filtering functionality and application programming interfaces to make it easier to procure and submit data to and from the system.

- Capability to quickly add or remove Compute, Storage, or Network resources to meet changing application needs and market volatility.

- Scalability to more efficiently meet historical data storage needs, provide data access through standard data services, and to respond quickly to regulatory requests.

- Secure, easy access to high-quality, high-fidelity data, including a centralized, enterprise-wide repository to store and provide timely access to system of record data.

Proposed Implementation Timeframe

OCC expects to launch the new core clearing, risk management, and data management applications into production no earlier than the second quarter of 2024. The proposed path to launch includes several milestones, such as connectivity testing in the first quarter of 2023, external environment testing in the second quarter of 2023, and certification of readiness from clearing members and exchanges in the first quarter of 2024.

Conclusion

OCC believes that the proposed cloud implementation meets the needs of the market participants we serve and is consistent with regulatory expectations and requirements. The proposed cloud implementation would provide OCC with a resilient, secure, and scalable environment to run core clearing, risk management, and data management systems that far exceed what is currently possible using only on-premises infrastructure. The cloud implementation will enhance OCC's ability to withstand and recover from adverse events by provisioning redundant Compute, Storage, and Network resources in three zones in each of two autonomous and geographically diverse regions. This will afford the OCC six levels of redundancy in the cloud with a primary and secondary virtual data center running in a hot (primary)/ warm (back up) configuration.

The proposed cloud implementation will ensure that OCC systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity. This would enable OCC to be more efficient and effective in meeting the requirements of its regulators, its participants and the markets it serves and promoting the stability of the broader financial system.