

## WHITEPAPER

---

### Author

Victor de Oliveira Pinto  
Senior Director

Yann Delacourt  
Director

---

### Contact Us

Americas  
+1.212.553.1658  
clientservices@moodys.com

Europe  
+44.20.7772.5454  
clientservices.emea@moodys.com

Asia (Excluding Japan)  
+85 2 2916 1121  
clientservices.asia@moodys.com

Japan  
+81 3 5408 4100  
clientservices.japan@moodys.com

---

## Regulatory Compliance as a Service

### The benefits of migrating regulatory compliance and regulatory reporting into the cloud

Over the coming years, risk and finance functions face an ongoing challenge to implement and update regulatory frameworks. The granularity, frequency, and widening scope of regulatory reporting is increasing the demand on technology infrastructure. Hosted architectures built on legacy systems ease that demand but do not provide a sustainable, scalable, high-quality solution. Thus, banks of all sizes are moving to a software-as-a-service (SaaS) approach: Regulatory Compliance as a Service (RCaaS). This option not only reduces costs but also provides superior levels of service and availability.

Moody's Analytics markets and distributes all Moody's Capital Markets Research, Inc. materials. Moody's Capital Markets Research, Inc. is a subsidiary of Moody's Corporation. Moody's Analytics does not provide investment advisory services or products. For further detail, please see the last page.

## Table of Contents

<b>Introduction</b>	<b>3</b>
<b>Total cost of ownership has been the main driver—until now</b>	<b>3</b>
<b>Multi-tenancy</b>	<b>4</b>
<b>Barriers to implementation are coming down</b>	<b>4</b>
<b>The case for moving regulatory compliance into the cloud</b>	<b>5</b>
<b>Why costs cannot be easily optimized on-premises</b>	<b>5</b>
<b>Software-as-a-service: The emphasis is on service</b>	<b>6</b>
Up and running fast	6
Instant regulatory updates	6
Performance	6
Agility	6
Community contributions	6
Transparent pricing	7
Security	7
Portability and reversibility	7
Domain expertise	7
<b>Alignment between banks, service providers, and regulators</b>	<b>7</b>
<b>Conclusion: The benefits of Regulatory Compliance as a Service</b>	<b>7</b>

## Introduction

For many banks and financial institutions, it is no longer a question of if they migrate applications and services to the cloud, but when, how, and in what order. This is a big decision, but many banks have already started the process. IT managers who continue to have doubts can easily find peers and third parties that have already blazed the trail and can share their knowledge and experience. In many countries, financial regulators are increasingly encouraging the use of cloud-based technology for regulatory reporting. The United Kingdom's regulator, and others, even provide a sandbox application for testing.

Regulatory compliance imposes high costs on banks and financial institutions, eroding profitability in the entire sector. Every round of regulatory updates calls for the rewriting of code and imposes more strain on IT infrastructures. In a recent Bank of England report, McKinsey & Company estimated that UK banks spend between £2 billion – £4.5 billion per year on regulatory reporting.<sup>1</sup>

### Total cost of ownership has been the main driver—until now

The main business driver behind the evolution of technology has always been cost, or more specifically, total cost of ownership (TCO). The cost of running and maintaining in-house developed applications has continued to grow exponentially. Around the turn of the millennium, many banks mitigated the high hardware costs of IT by transitioning their internally developed applications from expensive mainframe data centers to distributed client-server networks and web services—a process known as “rip and replace.” However, apart from the one-off cost of rip and replace, it did not address the issue of developing and maintaining software.

Banks often responded by investing in off-the-shelf software packages, paying an annual maintenance and support fee on top of the license. This had the advantage of reducing development costs but brought other drawbacks. Off-the-shelf third-party applications typically do not cover 100 percent of the requirements. For the remaining cost (assume 20–30 percent), banks must employ in-house developers or third-party consultancy firms, or pay the software vendor itself to customize its software to address specific needs. In this software deployment model, when the vendor issues a new release, the custom-built code no longer functions as it should, requiring further customization and maintenance. Consequently, upgrades could take months or even years to become stable.

Many banks have preferred to risk non-compliance and have delayed upgrades, losing competitive advantage from new enhancements. These institutions are not reporting based on latest regulatory rules, which triggers back-and-forth discussions with the regulator and poses potential non-compliance issues. Some face the operational risk of being insufficiently responsive following the latest changes.

A further downside to this business model is the license fee, which is payable regardless of how often the software is used, unused, or underused. Such applications are often referred to as “shelfware.” The 2011 Software Efficiency report found that shelfware accounted for £1.7 billion of wastage in the UK alone.<sup>2</sup>

In this context comes cloud computing. Cloud computing makes computer system resources, especially data storage and computing power, available by providing them on demand through the internet and without direct active management by the customer on local computers or servers.

When these resources include vendor-supported software applications that are accessible from client devices through either a thin client interface, such as a web browser or a program interface, this is called software-as-a-service (SaaS). With SaaS, the customer does not have to manage any of the IT infrastructure including network, servers, operating systems, storage, or individual application capabilities, except for limited user-specific application configuration settings.

Thus, a user organization such as a bank invests limited time and effort to configure a SaaS solution, as opposed to investing substantial amounts of time and effort to perform customization, do technical upgrades, and run the solution. Thereafter, upgrades and innovations fall entirely (or almost entirely) on the vendor. Because essentially identical resources are provided

---

<sup>1</sup> <https://www.bankofengland.co.uk/report/2019/future-of-finance>

<sup>2</sup> <https://www.silicon.co.uk/workspace/each-pc-holds-432-of-unused-software-26713>

by a single source as part of the “multi-tenant” arrangement, vendors can focus their efforts on development and innovation, rather than maintaining on-premises or legacy applications hosted on the cloud.

## Multi-tenancy

Multi-tenancy is a critically important concept. It enables vendors to offer the benefits of applications at a very low cost because these costs are shared. A vendor can serve multiple clients with a single version of its software (as opposed to hosting a different version of the software for each customer; that is, providing a single-tenant solution). This situation is similar to the electric power grid, in which a single power station supports thousands of households and businesses. Each customer is charged separately based on usage, but improvements to power-generation technology benefit all customers simultaneously. There are many examples of successful companies offering a SaaS solution as opposed to hosting, such as Salesforce.com, Workday, SuccessFactors, and Concur. Not only do they provide a higher level of service, but they do so at a fraction of the cost thanks to their multi-tenant architecture, which enables a pay-per-use pricing model.

The typical business model for SaaS is a usage-based subscription fee. There are other important concepts around SaaS computing that describe the benefits more precisely. These have been succinctly set out by the United States National Institute of Standards and Technology.<sup>3</sup> For “consumer,” substitute “user organization”:

**On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

**Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, tablets, laptops, and workstations).

**Resource pooling.** The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

**Rapid elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

**Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

## Barriers to implementation are coming down

Given all the advantages of cloud computing and SaaS, why have some banks been reluctant to go down this path? IT decision-makers in banks often point to security and privacy issues, especially given high-profile data breaches by hackers, or loss of data during data migration. Despite these barriers, attitudes are changing. Security measures in the cloud through multi-tenancy, including whitelisting and encryption of data in transit and at rest, all imply greater levels of sophistication, and are generally much better than in on-premises deployments. In addition, vendors have the specialized resources to implement and maintain multi-level security and strict isolation of data.

Consequently, this is no longer the number-one concern among IT leaders across all industries. In an IDG survey from 2018,<sup>4</sup> only 34 percent cited security as their main concern, down from 48 percent a year earlier. A similar number expressed their reluctance to move client data off-premises. The biggest concern now is “vendor lock-in,” although this is very much

---

<sup>3</sup> <https://www.nist.gov/>

<sup>4</sup> <https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/>

contingent upon the vendor's commercial strategy. Vendors that provide optimum service will have no trouble retaining customers without resorting to lock-in.

Further concerns include the following:

- » The ability of SaaS applications to integrate with in-house applications and data feeds
- » Compliance issues
- » The cost of the initial migration and the culture shift involved in relinquishing control
- » Organizations feel they lack the necessary skills to manage relationships with SaaS vendors

However, the barriers to cloud adoption are coming down. The same IDG report revealed that 73 percent of organizations have already adopted cloud technology and a further 17 percent intend to do so in the next year. That leaves just 10 percent who will delay adoption by one to three years. Moreover, many IT leaders are feeling the pressure to make or accelerate the transition. This is especially true in financial services, where 46 percent of IT leaders said they felt under pressure to migrate all IT applications to the cloud, compared to 38 percent across all industries.

### The case for moving regulatory compliance into the cloud

Looking at regulatory compliance, the case for moving applications off-premises and into the cloud in a SaaS configuration is more compelling than ever. First, the basic costs of on-premises software deployment are very high, in terms of hardware, network infrastructure, disaster recovery, and storage. However, these are only the visible costs, and many IT leaders could argue that subscription fees might be higher. Therefore, it is necessary to look at the TCO of remaining with on-premises deployment. Factors include the cost of software, the operating system, security monitoring, and the cost of managing and maintaining the solution in a context of constant regulatory changes.

Here are some examples of areas of the recurring costs of an on-premises approach, many of which are invisible or simply overlooked:

- » Hardware
- » Software licenses
- » Implementation/installation fees, including consulting fees
- » Support for existing software while installing new software
- » Creation of integrations and data exchanges between siloed applications
- » Testing solutions
- » Staff training and change management
- » Maintenance and support of systems and integrations
- » Non-IT functional resources (for example, HR or finance staff) to support on-premise solutions
- » Upgrade costs
- » Security, backup, and disaster recovery provisions
- » Cost of moving to next-generation technology

Banks that have visibility into these costs report that a SaaS approach can cut TCO by as much as half or two-thirds depending on their size and complexity, while their service improves dramatically. They benefit by scaling computing power according to need while ensuring high performance and availability.

### Why costs cannot be easily optimized on-premises

The cost of staying up to date with regulations is high. The rate of change in regulatory compliance may not stay at recent levels and fears of regulatory compliance costs doubling every few years might be overstated. However, there is no doubt about continuing, ongoing regulatory updates that require revalidation of regulatory compliance systems, imposing further costs. In addition, there are rapidly increasing volumes of data and a consequent need for added computational power; for example, many challenger banks would like to move from Basel's standardized risk weights to IRB, but this would require them

to perform more complex calculations on larger volumes of data. Likewise, the cost of quantitative impact studies (QIS) continues to rise.

To support such requirements in-house or even with a legacy solution hosted in the cloud requires an IT team that is organized to run new projects every year and retains the necessary expertise. Keeping this talent is challenging. It is expensive and there is little room to de-invest over time. Banks that attempt to cut costs risk compromising their ability to comply with new regulations and soon face an increasing operational and reputational risk.

### Software-as-a-service: The emphasis is on service

One of the more sustainable ways to reduce the costs of regulatory compliance is to choose a SaaS solution. This option lets banks exploit the benefits of multi-tenancy; for example, costs are shared by all the user organizations and payment is made on a per-usage subscription basis. Virtualization ensures a clear separation of data between these user organizations—they effectively have their own system running within the multi-tenant setup.

However, while SaaS does help reduce costs, this is only part of the story. Equally significant are the additional quality of service, speed of updates, and overall satisfaction to be gained, as long as the choice of service vendor is made carefully, and a service-level agreement is established that meets business requirements.

Here are some of the benefits that a SaaS solution provides in addition to lower TCO:

#### Up and running fast

Provisioning and on-boarding a new tenant in the system does not require a new infrastructure, so the services are available almost instantly, after a limited configuration exercise.

#### Instant regulatory updates

Regulatory changes can be applied immediately in a SaaS environment. Near-real-time software and regulatory upgrades with embedded non-regression testing tools make the process as transparent as possible. Tenants get streamlined access to new functionality, while bug fixes and end-user improvements are pushed automatically. All of this is transparent: users can see an impact analysis of any changes in a sandbox environment and decide whether they want to promote them or not. Additionally, there is a related cost-reduction aspect, as internal maintenance requirements are eliminated or significantly decreased.

Complexity is reduced by components that are used in several versions, such as Risk Weighted Assets under both Basel III and Basel IV, that are available in the same environment. Updates and additional features can be released without re-deploying the solution and incrementally deployed with no service interruption. Several versions co-exist.

#### Performance

In a SaaS environment, performance levels are tailored to match specific needs and priced accordingly. The level of performance can be increased for specific calculations for regulatory and for non-regulatory decision-making. For example, a SaaS solution could provide the computational power needed to run millions of risk scenarios in a short period of time; this is something that even the largest banks would struggle with using on-premises resources, but with a SaaS solution they can access scalable computing resources to realize the required performance. This scalability (or elasticity) is achieved through the distribution of a single application across various data centers to guarantee the highest standards in business continuity.

#### Agility

Using the power of a SaaS solution, it is possible to test new products more easily and bring them to market more rapidly and reliably. The same application is delivered instantly to subsidiaries or different legal entities thanks to a global cloud infrastructure. Banks can determine the data residency of choice for a particular entity, as the multi-tenant application is deployed globally.

#### Community contributions

Regulatory compliance is a cost, and not part of a bank's core business, so using a multi-tenant SaaS arrangement does not signify a loss of competitive advantage. On the contrary, new features and functionality as well as the standard solution can be made available through community contributions. This makes the banking and financial services industry as a whole more efficient and more profitable.

Alternatively, banks that make the most creative use of the additional computing power that a SaaS setup provides—for example, to gain additional insights through their own internal reporting—may secure competitive advantages.

### Transparent pricing

The costs of a SaaS solution are significantly lower. They are also more transparent and predictable, as they tend to be subscription-based, which benefits the user organization's financial planning.

### Security

With a SaaS solution supported by a cloud platform, banks get better security than on-premises operations. Security is multi-leveled, covering infrastructure, a virtual private cloud configuration, distributed denial of service mitigation, a range of data encryption options, inventory and configuration tools, monitoring and logging, identity and access control, and vulnerability and penetration testing.

### Portability and reversibility

A competent, reputable vendor will seek to retain customers through quality of service, not through vendor lock-in. Clients have the option to switch to another provider if they want to do so.

### Domain expertise

SaaS solutions are designed by, and for, domain experts who understand the regulatory frameworks and who anticipate future changes to get away from heavy reliance on IT. The value proposition is increasingly based on the users' ability to self-serve, for example, by identifying data that is required, and configuring and testing outputs for specific reporting requirements and scenarios. This is helped by the automation of many time-consuming tasks involved in extracting the data for specific regulatory frameworks and preparing it for analysis.

### Alignment between banks, service providers, and regulators

The latest guidelines require banks to comply but also to report on how they are complying with their respective regulatory authorities. It is vital to have a fully detailed and documented outsourcing arrangement. If banks cannot report on their outsourcing model, this can lead to penalties or the cancellation of the rights to operate.

Certain aspects of the bank's business continuity plan are transferred to the third-party cloud service provider, so there must be an assessment of the alignment between the bank's and the service provider's business continuity plans. The bank's internal auditors must be able to extend their reach to the cloud third party; therefore, public cloud service providers and SaaS vendors need to reach an agreement that brings all parties into alignment. Banks should build documentation into their process that shows evidence of the pre-outsourcing agreement. Plus, the SaaS provider must offer transparency and an exhaustive description of its internal security process and architecture.

### Conclusion: The benefits of Regulatory Compliance as a Service

The main user of any vendor's SaaS solution is the vendor itself. Improvements in engines, code, the upgrade process, technology utilization, and so on, simplify the vendor's administration of the solution, and attract new customers while retaining existing ones. This is generally the case with SaaS, but it is especially true with RCaaS. As barriers and objections gradually diminish, many of the world's larger banks and financial services institutions are opting for RCaaS. When costs are shared and come down, RCaaS also becomes the best option for small and medium-sized banks, which can see a rapid return on investment from reduced costs.

Hosted single-tenant solution providers cannot deliver these benefits. Banks and other financial services institutions probably see a slight reduction in costs and a slight improvement in service, but no more.

The Moody's Analytics technology roadmap is built on the cloud and puts service at the center of SaaS. Our roadmap addresses the main technical challenges faced by banks in the regulatory and finance environments: siloed applications, increasing data volumes, high and unpredictable costs, long project development times, and inflexibility in responding to evolving regulatory requirements. Banks can harness our expertise in regulatory reporting and our existing portfolio of applications to open source big data technologies. By offering a variety of cloud-native and cloud-hosted solutions—and empowering business users with self-service and automation of routine tasks—Moody's Analytics gives banks the ability to map their own journey toward scalable, high-performance, and affordable regulatory compliance.

© 2020 Moody's Corporation, Moody's Investors Service, Inc., Moody's Analytics, Inc. and/or their licensors and affiliates (collectively, "MOODY'S"). All rights reserved.

CREDIT RATINGS ISSUED BY MOODY'S INVESTORS SERVICE, INC. AND/OR ITS CREDIT RATINGS AFFILIATES ARE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MATERIALS, PRODUCTS, SERVICES AND INFORMATION PUBLISHED BY MOODY'S (COLLECTIVELY, "PUBLICATIONS") MAY INCLUDE SUCH CURRENT OPINIONS. MOODY'S INVESTORS SERVICE DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT OR IMPAIRMENT. SEE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S INVESTORS SERVICE CREDIT RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS, NON-CREDIT ASSESSMENTS ("ASSESSMENTS"), AND OTHER OPINIONS INCLUDED IN MOODY'S PUBLICATIONS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S PUBLICATIONS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. AND/OR ITS AFFILIATES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS DO NOT COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS, ASSESSMENTS AND OTHER OPINIONS AND PUBLISHES ITS PUBLICATIONS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS, AND PUBLICATIONS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS OR PUBLICATIONS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER.

ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS ARE NOT INTENDED FOR USE BY ANY PERSON AS A BENCHMARK AS THAT TERM IS DEFINED FOR REGULATORY PURPOSES AND MUST NOT BE USED IN ANY WAY THAT COULD RESULT IN THEM BEING CONSIDERED A BENCHMARK.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the rating process or in preparing its Publications.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING, ASSESSMENT, OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any credit rating, agreed to pay to Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it fees ranging from \$1,000 to approximately \$2,700,000. MCO and Moody's investors Service also maintain policies and procedures to address the independence of Moody's Investors Service credit ratings and credit rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold credit ratings from Moody's Investors Service and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at [www.moody.com](http://www.moody.com) under the heading "Investor Relations — Corporate Governance — Director and Shareholder Affiliation Policy."

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657 AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for Japan only: Moody's Japan K.K. ("MJKK") is a wholly-owned credit rating agency subsidiary of Moody's Group Japan G.K., which is wholly-owned by Moody's Overseas Holdings Inc., a wholly-owned subsidiary of MCO. Moody's SF Japan K.K. ("MSFJ") is a wholly-owned credit rating agency subsidiary of MJKK. MSFJ is not a Nationally Recognized Statistical Rating Organization ("NRSRO"). Therefore, credit ratings assigned by MSFJ are Non-NRSRO Credit Ratings. Non-NRSRO Credit Ratings are assigned by an entity that is not a NRSRO and, consequently, the rated obligation will not qualify for certain types of treatment under U.S. laws. MJKK and MSFJ are credit rating agencies registered with the Japan Financial Services Agency and their registration numbers are FSA Commissioner (Ratings) No. 2 and 3 respectively.

MJKK or MSFJ (as applicable) hereby disclose that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by MJKK or MSFJ (as applicable) have, prior to assignment of any credit rating, agreed to pay to MJKK or MSFJ (as applicable) for credit ratings opinions and services rendered by it fees ranging from JPY125,000 to approximately JPY250,000,000.

MJKK and MSFJ also maintain policies and procedures to address Japanese regulatory requirements.