

SECTOR IN-DEPTH

20 May 2026



TABLE OF CONTENTS

Leading AI models pose a heightened threat to the financial system	2
Cybersecurity spending is likely to rise, but companies can leverage AI too	3
Legacy architecture is the primary weakness	4
Moody's related publications	6

Contacts

- David Tao +1.212.553.3529
VP-Senior Analyst
david.tao@moodys.com
- Niclas Boheman +46.8.5179.1281
VP-Sr Credit Officer
niclas.boheman@moodys.com
- Lesley Ritter +1.212.553.1607
SVP-Cyber Credit Risk
lesley.ritter@moodys.com
- Leroy Terrelonge +33.1.5330.5989
VP-Sr Credit Officer
leroy.terrelonge@moodys.com

CLIENT SERVICES

- Americas 1-212-553-1653
- Asia Pacific 852-3551-3077
- Japan 81-3-5408-4100
- EMEA 44-20-7772-5454

Banks – Global

Arms Race: Deep defenses will help banks navigate cyber threats from new AI models

Cutting-edge AI models are accelerating the discovery of software vulnerabilities at a pace that outstrips the ability of most organizations to [patch them](#). Anthropic's Claude Mythos model, released to a limited number of organizations in early April, has autonomously identified thousands of previously unknown software flaws across every major operating system and web browser, marking a step change in the cyberthreat landscape. Anthropic has not released Mythos to the general public because of the severe cybersecurity risks it poses. The largest US banks were among an initial set of organizations given early access to the model as part of an initiative called Project Glasswing to allow them to test their cyber security defenses and detect software vulnerabilities. OpenAI released a similarly capable model called GPT-5.4-Cyber a week later, again to a limited number of organizations.

Banks and other financial institutions are prime targets for cyberattacks given the amount of customer funds and data held, the criticality of their payments infrastructure, the confidence-sensitive nature of their business, and their interconnectedness to the rest of the economy. AI developments are therefore particularly credit relevant for them. But banks' longstanding investment in [cyber resilience](#) and their regulatory discipline mean they are better positioned than most to defend against these threats. While the analysis in this report focuses on banks, the broader implications extend to other financial institutions, which face many of the same cyber risks but may have weaker cybersecurity defense.

- » **Leading AI models pose a heightened threat to the financial system.** The latest AI models are significantly better at detecting software vulnerabilities and pose increased risk to banks and the overall financial system if security and confidence in these institutions deteriorate. Larger institutions are bigger targets, but smaller ones are more vulnerable due to their more limited resources.
- » **Cybersecurity spending likely to rise, but companies can leverage AI too.** Heavy regulatory oversight of banks provides internal control discipline that contributes to more robust cyberdefenses than most companies, but smaller financial institutions with weaker controls or less resources likely need to increase cyber spending in order to properly defend against AI-enabled attacks. Nevertheless, all companies can leverage the new AI models for better self-defense through faster vulnerability detection.
- » **Legacy architecture is the primary weakness.** Outdated internal systems where software has not been patched for years are the most vulnerable to exploitation by cyber attackers. Patching should become more frequent and internal systems should operate on a zero-trust model to limit attackers' movements through the organization in the case of a breach.

Leading AI models pose a heightened threat to the financial system

Governments around the world have expressed concern that a technology as powerful as Mythos could pose a threat to financial stability.¹ As threat capabilities evolve rapidly, financial institutions will face increasing pressure to accelerate their response frameworks, reducing reaction times to detect, assess and contain AI-driven cyber incidents.

Leading AI capabilities around the world remain concentrated in the US and, to a growing extent, China. Most financial firms globally are consumers of cutting edge AI technology, creating a dependency on a small number of providers for both the offensive cyber tools that may be used against them and the defensive capabilities needed to protect themselves. While the credit implications are manageable for now, the pace of change will require banks to continue to treat cyber resilience as a strategic priority.

Large financial institutions have a broader attack surface area for network intrusion, but smaller institutions are more vulnerable from a defense preparedness and resource allocation perspective. According to IBM, the average cost of a US data breach is \$10.2 million - an all-time high.² With Mythos, the magnitude and sophistication of attacks are likely to increase, which could increase the total cost. Companies will need to fix their software vulnerabilities faster than malicious actors can exploit them.

These AI advances show the risk to banks is real and growing. Banks hold vast amounts of customer funds and data, maintain critical payments infrastructure, and operate complex IT systems. Failure to manage these responsibilities in a secure manner could lead to significant reputational damage and financial repercussions. For instance, a severe ransomware attack that disrupts services for an extended period could quickly become a threat to creditworthiness, potentially eroding confidence and liquidity.

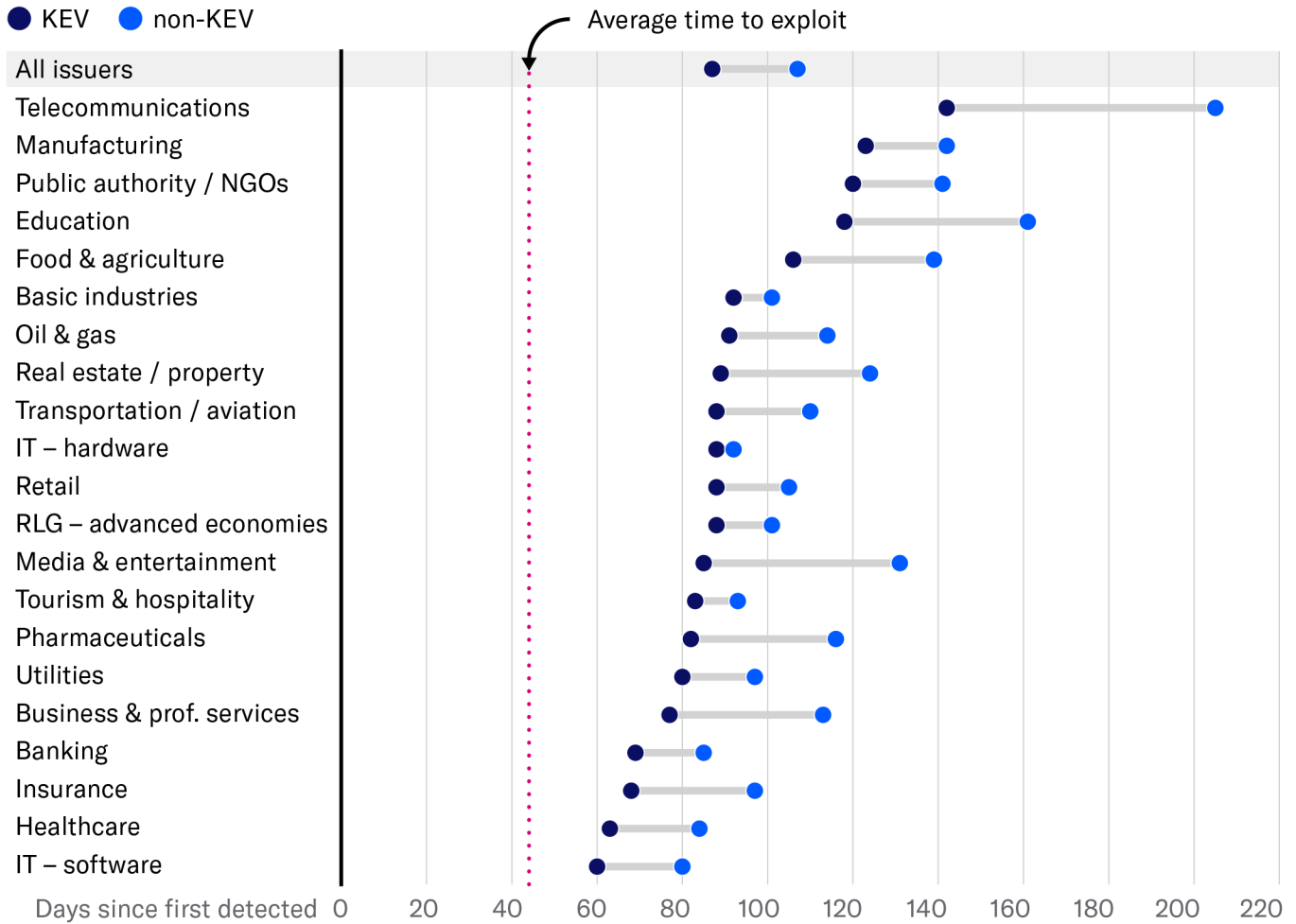
While software vulnerabilities are a leading cause of cyber breaches, phishing and other forms of social engineering targeting the human element also remain significant attack methods. According to Google research³, vulnerability exploitation was the single most frequent initial access method observed in 2024, responsible for roughly a third of confirmed network intrusions.

AI tools can uncover flaws faster than most organizations can remediate them. The gap between attacker speed and defender response is widening. According to Moody's [research](#), the average time for an attacker to exploit a software weakness fell to just 44 days in 2025, while median remediation times for such vulnerabilities was 87 days across all sectors. Banking sector remediation time was better at 69 days (see exhibit below):

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the issuer/deal page on <https://ratings.moody's.com> for the most updated credit rating action information and rating history.

Exhibit 1

Patching speed for financial institutions better than most sectors
 Median number of days to remediate vulnerabilities, by sector



Source: Moody's Ratings

Cybersecurity spending is likely to rise, but companies can leverage AI too

Banks are better positioned than most sectors to manage these risks. Our 2025 cyber [survey](#) of 228 banks worldwide⁴ found that banks follow more robust cybersecurity practices than other sectors. Nearly all the banks surveyed have adopted cyber vulnerability management programs and patch management policies, and the share allocating more than 10% of their technology budgets to cybersecurity continues to grow. Regulatory frameworks such as the EU's Digital Operational Resilience Act (DORA) or the Federal Financial Institutions Examination Council (FFIEC) operational resilience and cybersecurity framework in the US, enforce minimum standards for financial institutions across incident response, data backup and third-party risk management.

Financial institutions will need to increase spend to defend themselves. The impact as a percentage of revenues and profit will likely be smaller for larger banks with recently upgraded systems or that have moved to the cloud, but considerably larger for smaller firms with limited cost sharing structures. "Across industries, Bain estimates that "many organizations will need to significantly increase cybersecurity spending, by up to two times their current levels or even more; planned increases of about 10% annually fall far short of what the threat now demands."⁵ The overall cost will not just be in upgrading cybersecurity or hiring personnel. They will also need to patch or upgrade old systems and legacy technology, something that could pull resources away from new developments and revenue opportunities.

On the positive side, AI can be deployed by banks and other financial institutions to materially increase the speed at which software vulnerabilities and breaches are identified. However, these models do not provide ready-to-use remediation solutions, leaving banks to manage the complexity and execution risk of implementing fixes without disrupting interconnected IT systems. Institutions with more modern architectures and faster development cycles are therefore better positioned to adapt to the risks and opportunities presented by Mythos.

Furthermore, while the new AI models have accelerated the ability to discover software vulnerabilities, discovery alone does not equate to immediate exploitation. A hacker would still need to identify a viable attack path, gain the necessary access and successfully exploit the vulnerability. The gap between discovery and exploitation gives well-prepared defenders a critical window to act, reinforcing the value of rapid patching and layered security architectures.

The most durable approach to reducing software vulnerability risk is secure-by-design software development. This treats security as a core design requirement from the outset rather than a control added later in the development process. AI tools are increasingly supporting this shift by reviewing code changes for security flaws as they are introduced and suggesting safer alternatives aligned with best practices. Banks have a long track record of managing successive waves of technology-driven operational risk, and AI governance is advancing. Some 94% of respondents in our cyber survey said they had established formal AI usage policies.

Cyber risk is not an issue any single bank can address in isolation. Collaboration and information-sharing are central to how banks mitigate AI-driven cyber risk. Our survey reinforces this: 92% of banks participate in industry threat information-sharing groups, and 94% maintain service-level agreements with critical vendors requiring prompt notification of incidents or vulnerabilities.

Legacy architecture is the primary weakness

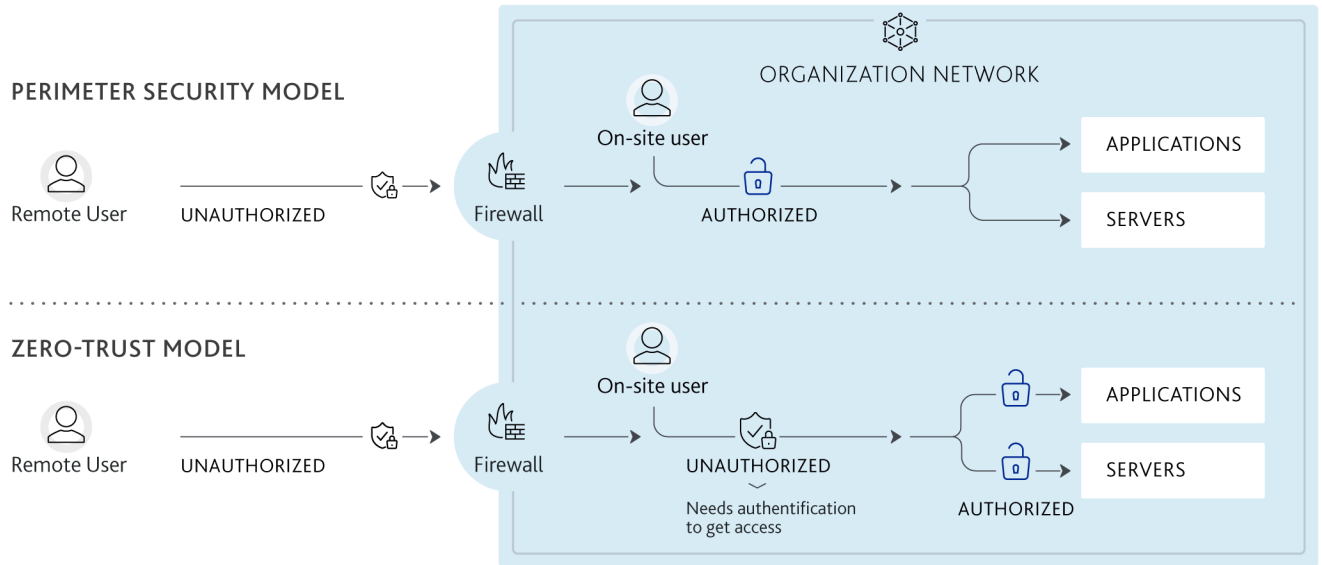
The capabilities of the new AI models will require banks and their cyber defense suppliers to work fast. Banks hold vast amounts of customer funds, maintain critical payments infrastructure and operate complex IT systems. While no single AI-driven software vulnerability discovery is likely to bring a bank down on its own, the cumulative effect of accelerating discovery-and-exploitation timelines raises the bar for remediation speed. A severe ransomware attack that disrupts services for an extended period could erode confidence and liquidity, underscoring the importance of proactive defense. As Mythos and models with similar or greater capabilities become more broadly available — as they almost certainly will — the pressure on remediation timelines will intensify. Static defenses requiring manual human input or monitoring that were used in the past are now likely to be insufficient.

Legacy IT infrastructure remains a key vulnerability for many financial institutions, with core banking systems in some cases dating back several decades. These environments are often complex and less adaptable, limiting the speed of upgrades, patching and incident response. While long operating histories are generally associated with stability, legacy systems may reduce resilience in the face of rapidly evolving AI-driven threats, increasing exposure to cyber risk.

Large networks of third-party vendors or software providers are another vulnerability. Almost every bank and financial institution uses third-party software, which offers another avenue for cyber perpetrators to enter a financial institution and cause disruption. Shrinking the footprint across vendors could help since a larger number of them increases the potential attack pathways.

In the new AI world, patching and security maintenance will need to be continuous. Periodic manual review by humans will likely be insufficient. Fortunately, banks are not staying idle - they have various monitoring [exercises](#) and put in control enhancements. For instance, Zero Trust architecture, which authenticates, authorizes and validates every access request, will be key to limiting the maneuverability of malicious actors once they breach corporate IT systems (see exhibit below):

Exhibit 2
Zero Trust vs Traditional Perimeter Security Model



Source: Moody's Ratings

Moody's related publications

- » [Risks posed by unpatched software flaws vary by industry and region, 1 April 2026](#)
- » [AI is uncovering software bugs faster than firms can patch them, 18 March 2026](#)
- » [Gaps in recovery capabilities increase vulnerability to a major cyber breach, 10 December 2025](#)
- » [Cybersecurity - North American financial institutions often at forefront; subset lags, 13 November 2025](#)
- » [Cybersecurity spending is growing as digital threats evolve, 25 September 2025](#)

Endnotes

- 1 https://www.nytimes.com/2026/05/04/technology/trump-ai-models.html?unlocked_article_code=1.gFA.56BW.G1Zok7tY0YO3&smid=url-share
- 2 <https://www.bain.com/insights/claude-mythos-and-ai-cybersecurity-wake-up-call/>
- 3 <https://services.google.com/fh/files/misc/m-trends-2025-en.pdf>
- 4 Representing \$46 trillion in aggregate assets
- 5 <https://www.bain.com/insights/claude-mythos-and-ai-cybersecurity-wake-up-call/>

© 2026 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 CREDIT RATINGS AFFILIATES ARE THEIR 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 OR OTHERWISE MADE AVAILABLE BY MOODY'S (COLLECTIVELY, "MATERIALS") MAY INCLUDE SUCH CURRENT OPINIONS. MOODY'S 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 APPLICABLE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S 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 MATERIALS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S MATERIALS 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 MATERIALS DO NOT CONSTITUTE OR PROVIDE LEGAL, COMPLIANCE, INVESTMENT, FINANCIAL OR OTHER PROFESSIONAL ADVICE, AND MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS 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 OR OTHERWISE MAKES AVAILABLE ITS MATERIALS 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 MATERIALS 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 MATERIALS 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. FOR CLARITY, NO INFORMATION CONTAINED HEREIN MAY BE USED TO DEVELOP, IMPROVE, TRAIN OR RETRAIN ANY SOFTWARE PROGRAM OR DATABASE, INCLUDING, BUT NOT LIMITED TO, FOR ANY ARTIFICIAL INTELLIGENCE, MACHINE LEARNING OR NATURAL LANGUAGE PROCESSING SOFTWARE, ALGORITHM, METHODOLOGY AND/OR MODEL.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS 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 or assessment 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 credit rating or assessment process or in preparing its Materials.

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 or assessment 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 Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it. MCO and all MCO entities that issue ratings under the "Moody's Ratings" brand name ("Moody's Ratings"), also maintain policies and procedures to address the independence of Moody's Ratings' 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, Inc. and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at ir.moody.com under the heading "Investor Relations — Corporate Governance — Charter and Governance Documents - Director and Shareholder Affiliation Policy."

Moody's SF Japan K.K., Moody's Local AR Agente de Calificación de Riesgo S.A., Moody's Local BR Agência de Classificação de Risco LTDA, Moody's Local MX S.A. de C.V., I.C.V., Moody's Local PE Clasificadora de Riesgo S.A., Moody's Local PA Clasificadora de Riesgo S.A., Moody's Local CR Clasificadora de Riesgo S.A., Moody's Local ES S.A. de CV Clasificadora de Riesgo, Moody's Local RD Sociedad Clasificadora de Riesgo S.R.L. and Moody's Local GT S.A. (collectively, the "Moody's Non-NRSRO CRAs") are all indirectly wholly-owned credit rating agency subsidiaries of MCO. None of the Moody's Non-NRSRO CRAs is a Nationally Recognized Statistical Rating Organization.

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 India only: Moody's credit ratings, Assessments, other opinions and Materials are not intended to be and shall not be relied upon or used by any users located in India in relation to securities listed or proposed to be listed on Indian stock exchanges.

Additional terms with respect to Second Party Opinions and Net Zero Assessments (as defined in Moody's Ratings Rating Symbols and Definitions): Please note that neither a Second Party Opinion ("SPO") nor a Net Zero Assessment ("NZA") is a "credit rating". The issuance of SPOs and NZAs is not a regulated activity in many jurisdictions, including Singapore. EU: In the European Union, each of Moody's Deutschland GmbH and Moody's France SAS provide services as an external reviewer in accordance with the applicable requirements of the EU Green Bond Regulation. JAPAN: In Japan, development and provision of SPOs and NZAs fall under the category of "Ancillary Businesses", not "Credit Rating Business", and are not subject to the regulations applicable to "Credit Rating Business" under the Financial Instruments and Exchange Act of Japan and its relevant regulation. PRC: Any SPO: (1) does not constitute a PRC Green Bond Assessment as defined under any relevant PRC laws or regulations; (2) cannot be included in any registration statement, offering circular, prospectus or any other documents submitted to the PRC regulatory authorities or otherwise used to satisfy any PRC regulatory disclosure requirement; and (3) cannot be used

within the PRC for any regulatory purpose or for any other purpose which is not permitted under relevant PRC laws or regulations. For the purposes of this disclaimer, "PRC" refers to the mainland of the People's Republic of China, excluding Hong Kong, Macau and Taiwan.

REPORT NUMBER 1483419

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454