MOODY'S
INVESTORS SERVICE

SECTOR IN-DEPTH
2 October 2019

Rate this Research

Contacts

Nisha Rajan +1.212.553.1978
Analyst
nisha.rajan@moodys.com

Leroy Terrelonge 1.212.553.2816
AVP-Cyber Risk Analyst
leroy.terrelonge@moodys.com

Orlie Prince +1.212.553.7738
VP-Sr Credit Officer/Manager
orlie.prince@moodys.com

Gregory W. Lipitz +1.212.553.7782
VP-Sr Credit Officer/Manager
gregory.lipitz@moodys.com

Leonard Jones +1.212.553.3806
MD-Public Finance
leonard.jones@moodys.com

CLIENT SERVICES

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

Local government – US

Ransomware attacks highlight importance of IT investment and response planning

As ransomware attacks increase in frequency and intensity, investing in IT infrastructure and personnel, establishing contingency plans and taking out cybersecurity insurance will help local governments reduce the impact of attacks on their operations and finances. Healthy reserve levels, access to short-term markets and state resources will also support municipalities' operations in the aftermath of attacks. Governments face a difficult decision over whether to pay ransoms. Paying will likely restore operations more quickly; not paying will sometimes lead to extended service disruption. Both scenarios will in most cases require additional expenditures, a credit negative.

» **Strong governance will play a major role in limiting the worst effects of ransomware attacks.** Municipalities that have dedicated IT staff or contractors to maintain system oversight and routinely test defenses are better equipped to deal with ransomware attacks. Additionally, cybersecurity insurance can provide organizations more options in responding to the effects of an attack.

» **Financial flexibility and state intervention also support municipalities' operations in the aftermath of attacks.** Local governments have so far largely withstood the financial impact of ransomware attacks, helped by generally healthy financial reserves and the ability to continue operations manually. But targeted ransomware attacks with higher ransom demands are becoming more commonplace, leaving smaller municipalities more vulnerable. Recent incidents in Louisiana and Texas highlight the benefits of support from state governments, which have access to more resources.

» **Local governments have a large degree of discretion in deciding whether to pay a ransom, a complicated calculus with a very involved payment process.** Ransomware victims must make a series of choices in determining whether to pay a ransom, including assessing the value of their data, the existence of backups or decryption keys and legal concerns. Paying will likely restore operations more quickly, while not paying sometimes leads to extended disruption of essential services. Ransom payments do not guarantee decryption, and oversight authorities warn against payment to deter funding criminal activities.

Strong governance plays a major role in limiting the worst effects of ransomware attacks

As ransomware attacks increase, strong governance will be credit positive for local governments, demonstrated by investment in IT infrastructure, implementation of strong cybersecurity practices and the purchase of cyber insurance. Such measures increase the speed, efficiency, and availability of resources, creating a pathway for responding to attacks. Many local governments choose to self-insure, to keep emergency reserves for unforeseen events like a cyberattack and to invest more heavily in personnel and infrastructure to bolster system resilience. Further, as local governments navigate through and recover from recent attacks, many are collaborating to share knowledge and lessons learned.

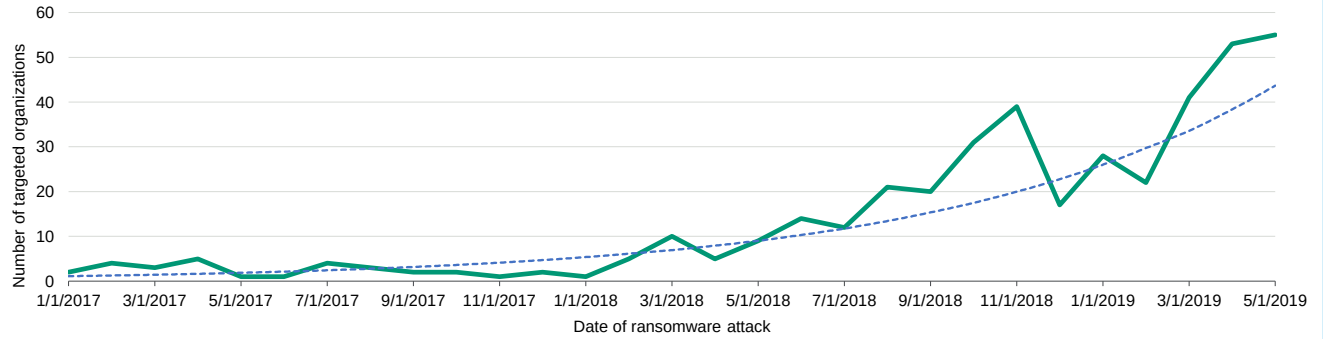
Reported ransomware attacks have increased sharply in recent years

Targeted ransomware attacks across all organizations and sectors increased markedly starting in early 2018, according to research by Symantec. While the company reported just one targeted attack in January 2018, it reported 55 in May 2019.[1] The US attracts the lion's share of targeted ransomware attacks globally: 900 between 2017 and 2019, compared with 100 during the same period affecting organizations in Turkey, the second-most affected country.

Reported ransomware attacks against local governments rose to 53 in 2018 from 46 in 2016, according to cyber threat intelligence firm Recorded Future, and in 2019 are likely to outstrip 2018 figures.[2] These figures reflect only reported attacks, and more have likely gone under the radar during this period.

Exhibit 1

Targeted ransomware attacks have sharply increased over the past two years



Organizations include all entities including public, private, academic, nonprofit etc.
Sources: Symantec; Moody's Investors Service

Following a 2018 cyberattack that crippled the computer systems of Matanuska-Susitna Borough (Mat-Su Borough, Aa2) in Alaska, borough managers mounted a rapid and coordinated response that involved protecting as much information as possible, maintaining essential services and revenue collection, and in the process minimizing reputational damage. With the borough reporting its computer systems restored to approximately 98% capacity by February 2019, the response highlighted how strong and active management in the wake of a breach can mitigate many of the risks associated with a cyberattack.

Orange County, NC (Aaa stable) actively invested in its infrastructure systems and software and was able to get most of its systems restored within 36 hours because of high-quality, up-to-date backups, following a ransomware attack in March 2019. The county's ability to restore operations and regain control quickly minimized additional costs and uncertainty, demonstrating the importance such long-term investments can have for local governments in the short run.

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the ratings tab on the issuer/entity page on www.moodys.com for the most updated credit rating action information and rating history.

States bolster oversight

States are also enhancing governance through controls and oversight to mitigate risk from cyberattacks. Over the last two years, for example, the State of Washington (Aaa stable) Auditor's Office (SAO) has offered three-pronged cybersecurity audits for local governments. These state-led cybersecurity audits are credit positive for Washington local governments because they help identify potential vulnerabilities, giving the municipalities an opportunity to mitigate threats before they materialize.

Furthermore, Nevada (Aa2 stable) and Montana (Aa1 stable) recently passed legislation establishing rules and frameworks for access to student data and disclosure of data breaches by third-party providers of K-12 school services. The laws demonstrate good governance of this issue and are credit positive for the state's school districts because many lack the resources and expertise to develop and enforce their own requirements.

Cyber insurance provides additional support for local governments

Cyber insurance provides organizations more options in responding to a ransomware attack. While policies vary, they can cover organizations for costs related to paying ransoms, hiring incident responders and purchasing new technology and equipment, which can significantly reduce the costs for victims of ransomware incidents. Mat-Su Borough, for instance, held a cyber insurance policy and received a payout, helping to curb financial losses.

Additionally, when Lake City, Florida (A1) faced a $460,000 ransom, it was only required to pay a $10,000 insurance deductible (approximately 0.1% of total operating revenues in fiscal 2018). The city's insurance company, the Florida Municipal Insurance Trust, covered the rest of the payment. The city then received a decryption key, enabling the restoration of operations.

Limiting financial impacts, however, are just one aspect of a successful response to ransomware incidents. Mature cybersecurity insurers also serve as facilitators for their customers, connecting ransomware victims with cybersecurity professionals who guide them through the recovery process. These services often result in materially improved outcomes for victims, especially given the time pressure in responding to ransomware attacks. Less-resourced organizations are more likely struggle to identify and connect with verified support services in a timely fashion.

Financial flexibility and state intervention also support municipalities' operations in the aftermath of ransomware attacks

The ability of cities, counties and school districts to absorb upfront financial costs and manually continue operations and services in the aftermath of a ransomware attack has meant the credit impact of such incidents has so far been negligible.

In May 2019, for example, a ransomware attack on Baltimore (Aa2 stable) hobbled city operations for nearly two months. In a separate, March 2018 incident, Atlanta (Aa1 stable) experienced a shorter disruption period of approximately two weeks when its systems were hit. Both cities elected not to pay the ransom demands to unlock their systems, reported at $76,000 for Baltimore and $51,000 for Atlanta. As a result, Baltimore paid short-term upfront costs more than of $18 million for replacement technology, personnel, and lost revenues. Costs associated with Atlanta's attack range from $10 to $15 million.

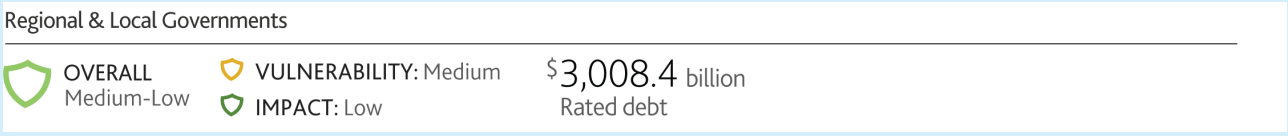
The estimated initial costs for both cities relative to their operating budgets and liquidity was minimal. In Baltimore, with a budget of $1.8 billion and cash reserves of $751 million in fiscal 2018, costs to restore its systems were less than 1% and 2.4% of revenues and liquidity, respectively. Relative to Baltimore, Atlanta's ransomware attack was more significant, but still manageable: the attack cost around 2.1% of its budget (approximately $700 million) and 7.2% of cash reserves ($209 million). Atlanta had also recently purchased cybersecurity insurance, a strong mitigating factor that resulted in full reimbursement for associated costs; Baltimore did not carry a cyber insurance policy. Further, both cities have quick access to liquidity through the short-term markets.

Both cities are regional economic hubs with substantial institutions, large budgets and diverse revenue streams, factors that also contributed to their quick recoveries.

Cyber risk for local and regional governments is medium-low

Although a rising challenge, our overall assessment of cyber risk for government entities is medium-low, driven by generally higher vulnerability scores that are mitigated by lower impact scores. Local governments nationally have increasing exposure to cybersecurity threats as they, along with businesses, nonprofits and government agencies at the state and federal levels, continue to aggregate data and move more services online. In recent years, local governments have been subject to several different kinds of cyberattacks, including ransomware, denial of service and breaches aimed at collecting sensitive and personal information.

The rate of digitization in these local and regional governments is generally lower than in higher-risk sectors. Where data is necessary for business processes, medium-low risk sectors are generally able to function with manual workarounds and sometimes benefit from some regulatory protections.



Ransomware attacks grow more sophisticated

As technology matures, however, methods for both infiltrating systems and demanding ransom payments are becoming more sophisticated and severe. Ransom amounts have ballooned from a few hundred dollars to tens of thousands of dollars to unlock an organization's computers, with some quotes now in the millions.

In July 2019, ransomware attackers demanded $5.3 million from New Bedford, MA (A1 stable), one of the highest sums to date, and a notable 17% of the city's fiscal 2018 cash reserves (yet just 1% of the overall budget). New Bedford countered with an insurance-backed payment of $400,000, which was rejected by attackers, thus yielding no ransom payment. The city is in the process of restoring systems by itself, aided by their sizable budget and insurance coverage.

Smaller, more vulnerable local governments benefit from state intervention

Smaller municipalities with limited resources, small budgets and lower liquidity are more vulnerable than larger local governments. They often have outdated technological systems and small IT budgets, and are limited in their ability to attract cybersecurity talent from an increasingly shallow pool. These factors also drive many local governments to contract out IT support and maintenance to third-party managed service providers (MSPs). While this structure provides certain benefits, notably cost savings, ransomware attacks targeting MSPs are also increasing, which can trickle down and infect local governments that use their services.

In August 2019, 22 entities across Texas, primarily smaller local governments, reported simultaneous and coordinated ransomware attacks. According to investigative officials, all were executed by a single malicious actor on one mutual MSP. The ransom demand neared $2.5 million, and so far neither the MSP nor the local governments have confirmed any ransom payments.

State support is a strong mechanism to help smaller local governments navigate the aftermath of an attack. In Texas, the state Department of Information Services and Division of Emergency Management pooled and deployed resources across state agencies to assist the affected entities, and all critical systems were reportedly restored within seven days. Similarly, Louisiana's governor declared a state of emergency in July 2019, when at least five of the state's school districts succumbed to ransomware infections in the span of a few days.

Local governments have a large degree of discretion in deciding whether to pay a ransom, a complicated calculus with a very involved payment process

While US law enforcement agencies recommend against paying ransoms, they do not generally prohibit or prosecute ransom payments, giving victims a large degree of autonomy in deciding whether to pay.

Local governments must weigh a range of considerations. Without access to critical data, municipalities may be unable to operate, frustrating customers and causing revenue loss. They may decide to pay a ransom because operations are at a complete standstill without doing so. Some may opt to pay because the turnaround time of regaining full network access with the decryption key is expedited and easier than relying on their own backups, and because the decryption key is not accessible through other means.

Jackson County, GA (Aa2 stable) paid $400,000 (0.6% of operating revenues and just 1% of their $40 million in cash reserves) in March 2019, when a ransomware attack locked down nearly all of its systems. The county did not have any backup systems in place, and the cost of rebuilding from scratch would have substantially outstripped the ransom amount, influencing management's decision to pay. As a result, the county gained access to a decryption key, which restored system access and reduced the time that services were inaccessible.

Paying a ransom does not completely shield a local government from the added expenses associated with incident response and recovery. Forensics experts are needed to determine the extent of the damage; purchasing and configuring new computer systems will cost money; and personnel will need to be paid for wiping, re-imaging and redeploying equipment.

The Federal Bureau of Investigation (FBI) and security researchers, as well as the US Conference of Mayors, advise not paying ransoms, for two primary reasons:

» **There is no guarantee of decryption.** Some ransomware variants are purposely coded without a decryption key. Others may contain bugs that prevent data from being recovered, even with the right decryption key. Cybercriminals also may demand additional payments or disappear once they receive the ransom payment. Still, attackers have an incentive to decrypt files. If large numbers of victims fail to receive decryption keys after paying ransoms, future victims will be less likely to consider paying. Accordingly, a 2016 joint study between anti-virus company Kaspersky and marketing company B2B International showed that cybercriminals provided victimized businesses decryption keys 81% of the time.[3]

» **Ransom payments fund criminal activities.** Paying ransoms encourages cybercriminals to continue their attacks on vulnerable and unprepared targets, in turn providing funds to develop and execute more sophisticated attacks.

Victims face a series of questions in deciding whether to pay a ransom

» **Is the ransomed data valuable?** Victims must decide if the ransom amount is commensurate with the value of their encrypted data. While it can be difficult to put a monetary value on data, municipalities can weigh the ransom amount against the cost of restoring operations from scratch (i.e. without their data). If it is cheaper to pay the ransom, the victim may choose to do so. If the victim has an insurance policy that covers ransomware attacks, this may shift the calculus by significantly lowering the cost of a ransomware payment. Additionally, cybercriminals have shown flexibility in negotiating ransom prices with victims.

» **Is there a backup for the ransomed data?** A data backup is one of the most powerful protections against a ransomware attack, and victims with a sufficient amount of critical data backups are unlikely to pay a ransom. To be effective, backups must be performed often (at least daily). Backups must also not be connected to the computers and networks they are backing up or they risk being infected during a ransomware attack.

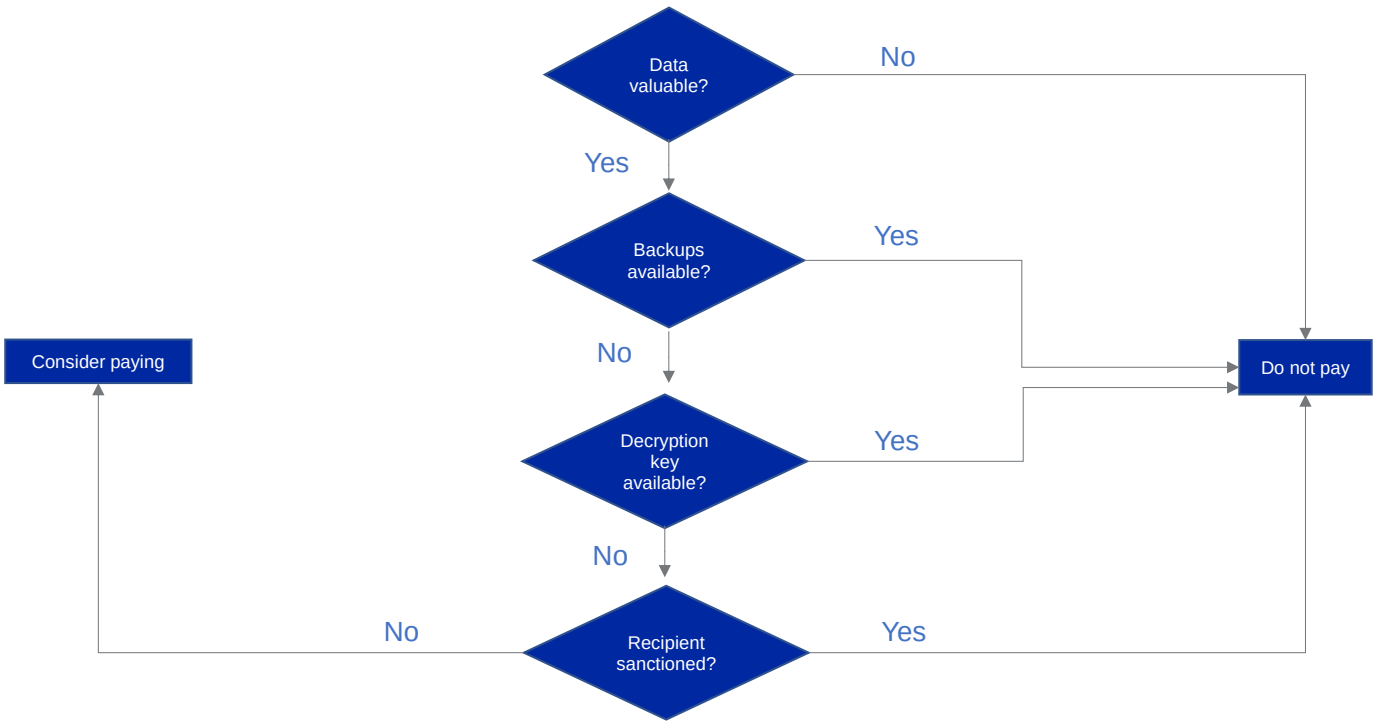
» **Is there a publicly available decryption key for the ransomware strain?**Decryption keys can help victims recover all or a portion of their data. Unfortunately, most ransomware victims cannot recover their data through technical means (for example, by reverse-engineering the encryption algorithm or writing a computer program to try every decryption key possible until the right one is found) because of the robust encryption protocols used in these attacks.

» **Is the extortioner a sanctioned entity?** While many law enforcement agencies generally tolerate ransomware payments, payments to sanctioned digital currency wallets could carry heavy penalties. Typically, victims do not know the identity of the criminals extorting them in a ransomware attack. But in November 2018, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) took the unprecedented step of adding two Iranian nationals to its list of sanctioned specially designated nationals (SDNs) for their alleged role in helping exchange Bitcoin ransom payments into Iranian rial on behalf of malicious ransomware actors. At the time of publication, the two Bitcoin wallet addresses associated with the SDNs are the only publicly announced digital currency sanctions globally. Given cybercriminals' penchant for using digital currencies, however, it is likely more addresses will be sanctioned in the future.

Exhibit 2

Ransoms: to pay or not to pay?

An illustrative decision tree of considerations faced by victims



Source: Moody's Investors Service

The payment process itself presents many difficulties

If a victim decides that paying a ransom is the best course of action, the payment process itself presents many hurdles:

» **Accessing the dark web.** Many ransomware variants require payment through a darknet technology (a network that requires specialized software for access) called the Tor network. Tor allows users to surf the regular internet (called the "Clearnet" to distinguish it from the darknet) anonymously, but also provides access to "onion services," servers configured to receive inbound connections only through the Tor network.

» **Maintaining a digital currency wallet.** To pay a ransom, victims must create digital currency wallets. Creating a digital currency wallet is simple and fast, but the tasks that follow are more complicated.

- *Trading limits*. Cybercriminals may give short deadlines for paying ransoms that range between several hundred thousand and several million dollars. Many popular exchanges, however, limit daily purchases of digital currencies to $100,000 or less, and require additional know-your-customer (KYC) verification procedures (address verification, proof of residence, government-issued identification, identification confirmation photograph, etc.) to execute a transaction. The time to process these checks may exceed the time allotted by the cybercriminals for their receipt of the ransom.
- *Volatility*. Digital currencies are notoriously volatile. The most widely used digital currency, one Bitcoin, went from trading at roughly $400 in January 2016 to trading at almost $20,000 in December 2017 before falling to $3,000 in December 2018. This variability can cause problems when paying ransoms. Cybercriminals generally demand ransom payments in the digital currency equivalent of a fixed fiat currency amount, thereby transferring the risk to the victim in the event of currency depreciation. The digital currency volatility also has tax implications, resulting in capital gains or losses, thereby creating increased compliance burdens.
- *Theft*. Digital currencies are common targets for cybercriminals, for both institutional (digital currency exchanges) and individual users. According to researchers, exchanges may have lost more than $1.2 billion because of theft, fraud and exit scams (administrators close an exchange and abscond with clients' funds) during just the first quarter of 2019. And cybercriminals have targeted individuals funds using malware, social engineering, and a technique called SIM-swapping that allows them to take control of mobile phone numbers and intercept login codes for digital currency wallets.

» **Engaging with criminal actors.** While some ransomware authors set up infrastructure for automated payment collection, others require victims contact them for payment details. Directly engaging with technically proficient criminal actors can expose victims to even greater risk, as the attacker can use the communication to learn more about the victim and leverage the additional information to inflict further damage. Experienced negotiators, however, can help victims save money.

Moody's related publications

Sector Comment

» Public K-12 school districts – US: State laws on student data collection by third-party vendors are credit positive, September 18, 2019

» State and local government – Louisiana: State-coordinated response improves school districts' outcomes in cyberattacks, August 07, 2019

» For-Profit and Not-For-Profit Hospitals – US: Hospitals invest in data collection, telemedicine to reduce cost, July 29, 2019

» Higher education – US: Cyberattack campaign underscores risks of using third-party services, July 25, 2019

» Local government - Washington: Washington State cybersecurity audits help mitigate risk from growing threat, August 14, 2018

Sector In-Depth

» Hospitals & health service providers - US: Cyberattacks pose growing operational and financial risks for hospitals, September 12, 2019

» Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 28, 2019

» Higher education - Global: Cybersecurity poses a growing credit risk in higher education, May 20, 2019

Issuer Comment

» Coconino County U.S.D. 1 (Flagstaff), AZ: Strong management, prudent approach to cybersecurity limit impact of ransomware attack, a credit positive, September 10, 2019

» Baltimore (City of) MD: Second ransomware attack in 15 months disrupts Baltimore's operations, May 28, 2019

» Matanuska-Susitna (Borough of) AK: Quick, coordinated response, access to emergency funds and insurance limit cyberattack losses, March 27, 2019

» Teton County School District 401, ID: Insurance will cover cybersecurity-related loss for Idaho school district, a credit positive, March 06, 2019

Endnotes

1 **Targeted ransomware: an ISTR special report**, Dick O'Brien, et al., Symantec, July 2019

2 **Early findings: review of state and local government ransomware attacks**, Allan Liska, Recorded Future, May 10, 2019

3 **Taking on ransomware**, Kaspersky, 2016

© 2019 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 ITS RATINGS AFFILIATES ("MIS") ARE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MOODY'S PUBLICATIONS MAY INCLUDE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES. 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 MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS AND MOODY'S 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. CREDIT RATINGS AND MOODY'S PUBLICATIONS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. NEITHER CREDIT RATINGS NOR MOODY'S PUBLICATIONS COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS AND PUBLISHES MOODY'S 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 AND MOODY'S 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 OR MOODY'S 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.

CREDIT RATINGS AND MOODY'S 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 the Moody's 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 OR 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 rating, agreed to pay to Moody's Investors Service, Inc. for ratings opinions and services rendered by it fees ranging from $1,000 to approximately $2,700,000. MCO and MIS also maintain policies and procedures to address the independence of MIS's ratings and rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold ratings from MIS and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at www.moodys.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 657AFSL 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 rating, agreed to pay to MJKK or MSFJ (as applicable) for 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.

REPORT NUMBER 1190715

CLIENT SERVICES

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

MOODY'S
INVESTORS SERVICE