RWR ADVISORY GROUP

SUPPLEMENTARY RISK PROFILE:

ANT TECHNOLOGY GROUP

September 25, 2020

Introduction

On August 25, 2020, Ant Group filed a draft "Application Proof" with the Hong Kong Stock Exchange (HKSE), ahead of what is expected to be the largest initial public offering (IPO) in history, with estimates that the listing will attract $30 billion or more.[1, 2, 3] An "Application Proof" is often referred to as a draft or preliminary prospectus and is part of the filing requirements that companies have to meet in order to proceed with a listing.[4] RWR released a report on September 6, 2020, describing various characteristics of Ant Group and its affiliates, as well as events in the company's history that could potentially lead to material and reputational risk for prospective investors.

Ant Group's "Risk Factors" section in its draft "Application Proof" submitted to the HKSE – or draft prospectus – exceeds 50 pages in length, but, in our view, air brushes over several material risk factors with the use of legal language that fails to convey a "plain English" description of the real world political, reputational and regulatory challenges the company could face in the period ahead. This approach may well protect the company and lead managers from charges of "material

[1] https://www1.hkexnews.hk/app/sehk/2020/102484/documents/sehk20082500535.pdf

[2] https://www.reuters.com/article/us-ant-group-ipo/ant-group-plans-to-raise-more-funds-in-shanghai-than-hong-kong-in-giant-ipo-sources-idUSKBN25T15U

[3] This report provides commentary on Ant Group's preliminary prospectus filed in Hong Kong as one part of the company's dual listing. Ant Group filed a separate application in Shanghai, which was accepted on September 18, 2020 and is subject to different regulations under a separate jurisdiction. All references in this report are solely to Ant Group's Hong Kong preliminary prospectus filing.

[4] The preliminary prospectus referenced in this report is Ant Group's draft "Application Proof," which is defined by the Hong Kong Securities and Futures Commission (the "SFC") as: "a substantially complete document at the time of Form A1 submission (except for information which by its nature can only be finalised at a later stage)." The "Application Proof" is published after passing a review by the Exchange and may be rejected by the Listing Committee up to the listing date, if the prospectus, including the "Risk Factors" section, is deemed inadequate.

risk omission," but it does not necessarily provide the fulsome brief that retail (individual) American investors require and deserve.

Without detailed knowledge of the overall risk environment related to the evolving bilateral U.S.-China relationship, the track record of risk that exists for Chinese technology companies dealing in sensitive user data is particularly troubling. This concern is exacerbated by the corporate governance system of the Chinese Communist Party (CCP). Prospective investors in the company's stock would be hard pressed to obtain an adequate understanding of the underlying material risk factors associated with Ant Group or its affiliates through a reading of the company's draft prospectus. Below, we seek to provide a "plain English" translation of Ant Group's characterizations of several of what we deem to be the most salient risk factors. This is an attempt to bridge the gap described above.

Failed MoneyGram Acquisition in the U.S.

Ant Group cites its 2018 attempt at a $1.2 billion acquisition of MoneyGram International, a Dallas-based digital payment and money transfer platform in the following manner (emphasis ours):

> "In addition, geopolitical tensions, protectionist or national security policies could, among other things, hinder our ability to execute our cross-border payment business strategies, make investments that develop new growth initiatives and technologies, or even divest from our current investees, and put us at a competitive disadvantage relative to local companies in other jurisdictions. *For example, in 2018, our attempt to acquire MoneyGram International Inc., a remittance company based in the United States, was not successful."*

What is missing from this technically accurate statement is any specific discussion of the underlying factors that led to the scuttled merger by the U.S. security community. For example, Ant Group fails to mention that the companies abandoned their filing for a required review by the Committee on Foreign Investment in the United States (CFIUS), after they were informed that clearance would not be forthcoming due to perceived national security risk.[5] Several lawmakers had earlier expressed concern over data privacy and national security risks stemming from the merger, citing Chinese government access to user information as well as the proximity of

[5] https://www.sec.gov/Archives/edgar/data/1273931/000119312518000668/d517771d8k.htm

MoneyGram's headquarters and money transfer agents to U.S. military bases and its use by many service members to send remittances home.[6, 7]

Role in Mass Detention and Surveillance in the Xinjiang Uyghur Autonomous Region

Ant Group and Alibaba are both sizeable investors in, and customers of, Megvii Technology, an artificial intelligence (AI) startup that specializes in facial recognition technology. Megvii was sanctioned by the U.S. Government and added to the Entity List of the Commerce Department's Bureau of Industry and Security (BIS) in October 2019 for having been "implicated in human rights violations and abuses in the implementation of China's campaign of repression, arbitrary detention, and high-technology surveillance in the XUAR."[8]

The entirety of Ant's related risk disclosure in its draft prospectus is as follows (emphasis ours):

> "The United States has also threatened to impose further export controls, sanctions, trade embargoes, and other heightened regulatory requirements on China and Chinese companies for alleged activities both inside and outside of China. These have raised concerns that there may be increasing regulatory challenges or enhanced restrictions against China and other Chinese technology companies, including us and Alibaba, in a wide range of areas such as data security and privacy, emerging technologies, "dual-use" commercial technologies and applications that could be deployed for surveillance or military purposes, import/export of technology or other business activities.
>
> For instance, in 2019 and 2020, the U.S. government announced several executive orders and regulations effectively barring American firms from selling, exporting, re-exporting, or transferring U.S.-origin technology, components and software, among other items, to Chinese technology companies, including Huawei Technologies Co., Ltd., and their respective affiliates. Companies that have been targeted by such export restrictions, and can no longer obtain much U.S.-origin technology, components and software, *including Megvii Technology Limited, in which we hold a minority interest."*

[6] https://www.wsj.com/articles/check-chinas-financial-investments-in-the-u-s-1487700633
[7] https://www.washingtonpost.com/news/josh-rogin/wp/2017/07/19/chinas-jack-ma-has-penetrated-the-trump-administration-and-he-knows-what-he-wants/
[8] https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list

Via this language, Ant Group identifies the risk of export controls and sanctions and the impetus for such regulatory actions, including the potential application of technology for "surveillance or military purposes." The risk section, however, omits reference to the purpose of the U.S. government's recent actions against Chinese technology companies, including Megvii, which is their role in human rights violations and the implementation of China's campaign of repression in Xinjiang.[9] The disclosure also fails to describe the depth of the international outrage that exists on this very topic and the pressure that companies are coming under for their perceived complicity in it. There is also only limited, technically worded treatment of the proliferation of these concerns to other areas of Chinese jurisdiction or even third-party countries, where China's model of "surveillance state" technology solutions are taking root.

Chinese Government and CCP Ties and Influence

Ant Group devotes significant space in its draft prospectus to a description of the Chinese legal code and economic structure. While technically accurate, a recounting of China's tax laws does not, in our view, adequately inform prospective investors of the material risks associated with the nature of China's authoritarian, single-Party government involvement in Ant Group and its affiliates. An excerpt of Ant Group's characterization of its relationship with the Chinese Government in its draft prospectus appears below (emphasis ours):

> "A substantial portion of our businesses, assets and operations are located in China. Accordingly, our financial condition, results of operations and business prospects are, to a significant degree, subject to the economic, political and legal developments in China. China's economy differs from the economies of most developed countries in many respects, including, among other things, government involvement, level of economic development, economic growth rate, control of foreign exchange and allocation of resources. China's economy was a planned economy, and a substantial portion of productive assets in China is still owned or controlled by the PRC government.
>
> The government also exercises significant control over China's economic growth by allocating resources, setting monetary policy and providing preferential treatment to particular industries or companies. Although the government has implemented economic

[9] https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list

> reform measures to introduce market forces and establish sound corporate governance in business enterprises, the application of such economic reform measures may vary from industry to industry, or across different regions of the country. As a result, we may not benefit from certain of such measures."

First, it is worth pointing out that nowhere in the draft prospectus is there reference to the Chinese government being ruled by the Communist Party of China (CCP), whose party structures play an integral role in the government's control and involvement being referenced by this language. In this connection, Ant Group's ties to the Chinese government include: 1) mandatory "Party building" initiatives that require the creation of CCP cells and/or "working groups" within senior management structures; 2) contracts and agreements between the company and several municipal governments and government entities; and 3) implementation of the CCP's internet policies and regulations, a particularly significant factor in the fintech industry.

Ant Group's founder and majority shareholder, Jack Ma, has referenced the company's government ties in interviews. On the one hand, he has insisted, in trying to defend the independence of the company, that Ant Group will "only fall in love with the government and never get married." On the other, he has made clear that "As long as the country needs it, we are ready to dedicate Alipay to the country at any time."[10]

Military Dual-Use Potential

As noted above, Ant Group discloses in its draft prospectus the possibility that its business may be affected by,

> "…enhanced restrictions against China and other Chinese technology companies, including us and Alibaba, in a wide range of areas such as data security and privacy, emerging technologies, 'dual-use' commercial technologies and applications that could be deployed for surveillance or military purposes, import/export of technology or other business activities."

This acknowledgement of technologies that "could be deployed" in military capacities appears to be a reference to China's vast military-industrial complex, which integrates civilian and military technology for national defense purposes. Specifically, China leverages big data

[10] https://v.qq.com/x/page/f05063v2xbg.html

aggregation and processing capabilities to advance, for example, military intelligence-gathering and analysis. Alibaba was previously mentioned by the U.S. government in the context of China's military-civil fusion program and the risk exposure it presents to private sector actors doing business with them.

Specifically, on September 11, 2019, Christopher Ashley Ford, U.S. Assistant Secretary of State for International Security and Non-Proliferation, discussed in a speech the implications of engaging with Chinese technology giants, including Alibaba Group. He noted that military-civil fusion means that,

> "Military-civil fusion also means that it is very difficult and in many cases impossible to engage with China's high-technology sector in a way that does not entangle a foreign entity in supporting ongoing Chinese efforts to develop or otherwise acquire cutting-edge technological capacities for China's armed forces."[11]

He also noted,

> "According to a December 2018 article published on the National Military-Civil Fusion Public Platform administered by the Ministry of Industry and Information Technology, products and technologies from Huawei, Tencent, Alibaba, Xiaomi, Lenovo, and other companies have already been used in the research, production, and repair of weapons and equipment for the PLA. These companies have also provided support services for China's military industry in areas related to electronics, aerospace, shipbuilding, and weapons — all of which, incidentally, are key military-civil fusion target areas when it comes to foreign technology acquisition — to enhance the core competitiveness of China's national defense science and technology sectors."[12]

[11] https://www.wsj.com/articles/china-taps-its-private-sector-to-boost-its-military-raising-alarms-11569403806
[12] https://china.usc.edu/christopher-ford-state-department-huawei-and-its-siblings-chinese-tech-giants-national-security-and

Participation in Social Credit System Construction

Ant Group does not make any reference to the participation of its subsidiary, Zhima Credit Management (Sesame Credit) as one of eight companies selected for the 2015 construction of a private credit scoring program, facilitated by the People's Bank of China (PBOC), which was intended to supplement China's state-run personal credit database.[13]

The database, derived from large-scale data collection and analysis, reportedly assigns scores to citizens based, not just on their economic reputations, but also on their social track records.[14] Due to inconsistencies between the credit scores generated by the eight companies, perceived overreach by leading provider Zhima Credit, and concerns about a potential credit data oligarchy, PBOC revoked their permissions in February 2018 and instead made all of them shareholders in a new unified personal credit information platform known as Baihang Credit Scoring.[15] This involvement or proximity to a system of CCP control over its citizens, which has been widely scrutinized and criticized by outside observers as Orwellian in nature, strikes us as potentially "material" to the risk-related decision-making of prospective investors.

Data Collection and Privacy Concerns

Ant Group, like other companies operating in the fintech and digital payments sectors, faces significant cybersecurity risk as a core arbiter of payments made on the Alipay platform and the custodian of sensitive personal and financial data on millions of users. Investors reading Ant Group's draft prospectus without knowledge of the company's poor data privacy track record – which includes an accusation by China's cyber watchdog, the Cyberspace Administration of China (CAC), that the company failed to meet national security standards for personal information in 2018 – would remain in the dark concerning this category of risk.[16] The draft prospectus instead provides a list of "challenges relating to data security and privacy" related to the fintech industry, acknowledging that:

> "There are also uncertainties with respect to the laws and regulations related to data security and privacy in the PRC. Regulators in the PRC, including MIIT and the

[13] https://www.piie.com/system/files/documents/pb18-1.pdf
[14] https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590
[15] http://www.xinhuanet.com/english/2018-02/22/c_136991905.htm;
[16] https://www.caixinglobal.com/2018-01-11/ant-financial-to-review-privacy-policy-after-receiving-slap-on-wrist-101196761.html

> Cyberspace Administration of China, have been increasingly focused on regulation in the areas of data security and privacy. We expect that these areas will receive greater and continued attention and scrutiny from regulators and the public going forward, which could increase our compliance costs and subject us to heightened risks and challenges associated with data security and data protection…
>
> In addition, in July 2020, the Standing Committee of the National People's Congress of China released the draft data security law for public comment ('Draft Data Security Law'). The Draft Data Security Law provides that a classified data protection system will be applied based on the level of importance of the data and at the national level a centralized mechanism for risk assessment, monitoring, and early warning of potential data security risks and emergency response will be established. The Draft Data Security Law also provides for the data security and privacy obligations on entities and individuals carrying out data activities. As the Draft Data Security Law remains subject to change, we may be required to make further adjustments to our business practices to comply with the enacted form of the law."

In our view, the mere acknowledgement of "uncertainties" around Chinese cybersecurity laws, while probably constituting legally required risk disclosure, is not a sufficient substitute for a discussion of the data privacy risks facing Ant Group due, not only to its poor track record, but, more importantly, to its ties to the CCP and exposure to Chinese laws that mandate cooperation with the CCP in a variety of instances. These misgivings have been echoed by foreign governments, including India, which earlier this month banned Alipay and 117 other Chinese-owned or -linked apps over data privacy concerns.[17] The U.S. government has also repeatedly highlighted the risks associated with engaging with Chinese technology companies that have access to personal data due to concerns with regard to how such data might be accessed and used by the CCP.

[17] https://www.scmp.com/abacus/tech/article/3029480/facial-recognition-payments-are-privacy-risk-says-china-central-bank

Vulnerability to Escalating Geopolitical Tensions

Ant Group includes in its risk disclosure a section on the effects of deteriorating U.S.-China relations, including potential sanctions and export restrictions that could affect Ant Group or any of its subsidiaries/partners. The two pages (beginning on page 44) devoted exclusively to U.S.-China geopolitical risk can be broken down into a detailed description of the recent executive orders relating to ByteDance, WeChat, and Tencent Holdings Ltd., a description of U.S. sanctions in general, and recognition of the uncertainties surrounding the future of China's relations with other countries. Excerpts appear below:

> "These restrictions, and similar or more expansive restrictions that may be imposed by the U.S. or other jurisdictions in the future, may materially and adversely affect our ability to acquire or use technologies, systems, devices or components that may be critical to our technology infrastructure, service offerings and business operations; to access U.S. cloud-based systems and other infrastructure; and to operate in the U.S. In addition, these policies and measures directed at China and Chinese companies could have the effect of discouraging U.S. persons to work for Chinese companies, which could hinder our ability to hire or retain qualified personnel to work for our business. We cannot assure you that the current export controls or economic, trade or other sanctions regulations will not have a negative impact on our business operations or reputation, or that the related trend will not further deteriorate in the future. Furthermore, policies of the United States tend to be followed by certain other countries, and these countries may adopt similar policies regarding their relationships with China or against Chinese companies and restricting their operations…
>
> Separately, media reports on alleged violations of applicable export controls, economic and trade sanctions, or data security and privacy laws, or on uses of the technologies, systems or innovations that we develop for purposes which could be perceived as inappropriate or controversial, by us, merchants, partner financial institutions and other participants on our platform, even on matters not involving us, could nevertheless damage our reputation and lead to regulatory investigations, fines and penalties against us…
>
> Any further escalation in trade or other tensions between the United States and China or news and rumors of any escalation, could introduce uncertainties to China's economy and the global economy, which in turn could affect activity level on our platform."

Regarding the material geopolitical risks facing Ant Group, and other publicly traded Chinese multinationals, investors reading Ant Group's "Risk Factors" section are provided with a legalistic explanation of general geopolitical trends, and a perfunctory disclaimer of uncertainty as to how exactly these trends will likely materialize, and the potential effects on Ant Group's business. Both the pace of decoupling and the scale of bipartisan concern in the United States relating to China, present, in our view, a much more challenging picture for Ant Group's operations than is implied by the legalistic explanation of general geopolitical trends provided in the company's draft prospectus.

Concerning regional geopolitical risk, the draft prospectus states:

> "Separately, in 2020, a change in foreign investment regulation in India led to our further evaluation of the timing of our additional investment in Zomato [in which Ant Group holds a 25% stake], a restaurant aggregator and food delivery start-up based in India."

Upon additional, independent research, the prospective investor would learn that, in fact, a military standoff on the Chinese-Indian border in June resulted in the deaths of 20 Indian soldiers, sparking a protest by Zomato workers in Kolkata, who burned their uniforms and were reportedly heard chanting, "Indian army soldiers have been killed, but Zomato loves China."[18]

Disclaimer

This document is intended for general informational purposes. RWR disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information.

RWR does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals. This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

[18] https://www.ft.com/content/b1df5dfd-36c4-49e6-bc56-506bf3ca3444