RWR
ADVISORY GROUP

RISK PROFILE: ANT TECHNOLOGY GROUP

September 6, 2020

Summary of Risk Factors

1. Failed MoneyGram Acquisition in the U.S
2. Role in Mass Detention and Surveillance in the Xinjiang Uyghur Autonomous Region (XUAR)
3. Military Dual-Use Potential
4. Participation in Social Credit System Construction
5. Data Collection and Privacy Concerns
6. Chinese Government Ties and Influence
7. Vulnerability to Escalating Geopolitical Tensions

Background

Ant Technology Group (Ant Group), formerly known as Ant Financial Services Group, is a partially owned (33%) subsidiary of Chinese e-commerce giant Alibaba Group Holding (BABA: NYSE) that primarily provides financial technology (fintech) products and services. The company's recent name change (in June 2020) has been characterized as intended to reflect better its transition from a financial services provider to a global technology provider that connects businesses across industries.[1]

Of Ant Group's 1.2 billion users, the vast majority (900 million) reside in mainland China, where the company's estimated $150 billion market capitalization is derived from a 53.8% share of China's mobile payment market. Ant Group's Alipay payment platform is active in 50 countries, supports 27 currencies, and currently maintains partnerships with over 250 overseas financial institutions and payment solution providers that primarily support Chinese travelers and foreign customers using Chinese e-commerce sites. In contrast, Ant Group's largest competitor PayPal serves 346 million active users across 190 countries and supports 25 currencies, with about 4 million U.S. users.[2] PayPal's valuation at the time of its IPO in 2015 was $46.6 billion.

Industry Leadership

Ant Group and Alibaba are based in Hangzhou, the capital city of Zhejiang Province. Hangzhou is a major hub for China's financial technology industry and is considered the "capital of Chinese e-commerce." According to municipal government guidelines issued in May 2019, Hangzhou seeks to become a global fintech leader, which it says it is doing through pledged policy guarantees, intellectual support, and talent resources. Hangzhou's efforts to nurture a technology industry are bolstered by its proximity to the Qiantang River Financial Harbor and the Hangzhou West Science and Technology Corridor, as well as its participation in the "Thousand Talents" recruitment program that brings overseas high-level specialists to the city.[3] Like other of China's "innovation" hubs, however, the regional industry – and the government's role in fostering it –

[1] https://www.wsj.com/articles/jack-mas-fintech-giant-ant-to-drop-financial-from-its-name-11592822997?mod=tech_lead_pos2
[2] https://www.axios.com/alibaba-alipay-america-expansion-walgreens-118df09f-55f6-425f-b3e7-d5a77ccf1a5e.html
[3] https://news.caijingmobile.com/article/detail/396538?source_id=40

exists under the shadow of allegations of a protracted, multi-decade effort by Beijing to acquire foreign technology and intellectual property via theft and coercion.

Ant Group is a leader in the fintech industry in Hangzhou, which ranks second only to Beijing as the Chinese city with the highest number of blockchain companies. Moreover, Hangzhou was even selected by the UN International Telecommunication Union's (ITU) Digital Currency Laboratory to host its Chinese headquarters.[4] The world's first blockchain-based electronic wallet cross-border remittance service was launched in Hong Kong in June 2018 using Alipay HK (a wholly owned subsidiary of Ant Group) and Hangzhou launched the country's first blockchain electronic seal platform through AntChain in July 2020.[5]

Ant Group's main advantage in this field has been attributed to its qualification as the company with the largest number of blockchain patents in the world and its resulting ability to provide Ant Group's Ant Financial Blockchain platform with a robust technical support team.[6] The company's domestic market share (described above) and its relationship with the Chinese government, however, also denote the favor with which the company is viewed by Beijing, another asset serving the company in the international market place.

Financial and Fiduciary Risk Factors

Ant Group filed its prospectus with the Hong Kong Stock Exchange on August 25, 2020, ahead of what is expected to be the largest initial public offering (IPO) in history. The company's public valuation is currently estimated at $225 billion.[7] In one of its filings, Ant disclosed that it plans to sell shares worth at least 10% of its share capital, suggesting that the IPO could attract up to $30 billion or more, according to recent reporting.[8] Ant Group will list an undisclosed number of H-Shares and A-Shares on the Hong Kong and Shanghai Stock Exchanges, respectively. The IPO is being managed by China International Capital Corporation (CICC) and American firms

[4] https://news.8btc.com/chinas-first-itu-digital-fiat-currency-lab-is-established-in-hangzhou
[5] https://www.chainnews.com/articles/734317580773.htm
[6] https://technode.com/2020/07/03/alibaba-leads-global-blockchain-patent-but-china-lags-behind-us-and-s-korea/
[7] https://www1.hkexnews.hk/app/sehk/2020/102484/documents/sehk20082500535.pdf
[8] 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

Citigroup, JP Morgan Chase, Morgan Stanley and, as per reports published on September 5, Goldman Sachs as the joint lead managers.[9]

The predicted magnitude and potential profitability of the IPO has drawn substantial interest from U.S. investors, who will be able to access the company's A Shares and H Shares through their reportedly imminent inclusion in emerging markets and international indexes and, as a result, those Exchange-Traded Funds (notably those managed by Black Rock and Vanguard) and other financial products that benchmark against these indexes.

According to the Center for Financial Research and Analysis, however, U.S. investors will likely gain first exposure to Ant Group securities through Renaissance Capital's International IPO ETF.[10] Analysts expect an expedited timeline for the company's inclusion in other major ETFs, such as the Vanguard FTSE Emerging Markets and the iShares Core MSCI Emerging Markets ETFs, given the size and liquidity of Ant Group. As a result, Ant Group is on track to benefit substantially from inclusion in these U.S. indexes, tracked by trillions of dollars in ETFs, despite national security concerns keeping the company, in other circumstances, from making inroads into the U.S. economy, most notably demonstrated in the failure of its planned acquisition of American digital financial services company MoneyGram International in 2018.

Ant Group's Hong Kong Stock Exchange prospectus discloses potential financial technology and e-commerce sectoral risks, but largely glosses over other important risk factors that potentially threaten the firm's corporate reputation, such as the company's ties (through ownership and business involvements) with the Chinese Communist Party (CCP). In our view, it also inadequately addresses the national security- and human rights-related risks associated with data security and privacy concerns (the 55-page "Risk Factors" section of the prospectus begins on page 30).[11]

Moreover, some observers have suggested that Ant Group's decision to go public in Hong Kong and Shanghai stems from Beijing's concern over the significant bipartisan political activism that has developed over the past year related to China's corporate presence in the U.S. capital markets, which has been led both by the Congress and the Trump Administration.

[9] https://www.bloomberg.com/news/articles/2020-09-05/ant-is-said-to-hire-goldman-sachs-as-joint-lead-manager-for-ipo?sref=x6YSiRFO
[10] https://www.cnbc.com/2020/07/24/ant-financial-ipo-using-etfs-to-play-the-historic-dual-listing.html
[11] https://www1.hkexnews.hk/app/sehk/2020/102484/documents/sehk20082500535.pdf

Some of the issues of concern to these policy-makers during this period appear present in Ant Group, such as the right that the company maintains under Chinese law, despite not being technically state-owned, to avoid disclosing financial information. Ant Group's dual listing in Hong Kong and Shanghai would appear to situate the company outside of the purview of the U.S. government's Public Company Accounting Oversight Board (PCAOB) and its periodic inspections of audits. Even for Chinese companies actually listing in the U.S. capital markets, however, China has routinely interdicted the PCAOB's efforts to review Chinese auditing procedures, which are otherwise mandatory under U.S. securities laws (e.g., the Sarbanes-Oxley Act).[12]

In the absence of PCAOB oversight (as the company will not be U.S.-listed), American investors in the company following the IPO – through both passive and active investment vehicles – could well be subject to an elevated, if not undue, level of risk. In short, Ant Group's IPO falls within a larger pattern of Chinese enterprises that, to the detriment of American investors, have been permitted entry into the U.S. capital markets without having to provide comparable levels of disclosure and transparency required of their U.S.-based corporate counterparts.

This leaves to Beijing's discretion decisions concerning what parts of a company's financials are considered national security concerns and therefore off-limits to U.S. investors and regulators. Addressing this long-standing, preferential regulatory treatment accorded China by the Securities and Exchange Commission will likely call for fiduciaries to perform more comprehensive and deeper diligence and exercise enhanced fiduciary responsibility, neither of which are in evidence today.

Risk Factors

1. Failed MoneyGram Acquisition in the U.S.

In 2018, Ant Financial attempted a $1.2 billion acquisition of MoneyGram International, a Dallas-based digital payment and money transfer platform. The deal collapsed after 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

[12] https://pcaobus.org/International/Pages/China-Related-Access-Challenges.aspx

perceived national security risk.[13] The acquisition would have granted Ant Financial access to the entirety of MoneyGram's mobile user accounts, as well as its $2.4 billion bank.

- Given that the Chinese government owns an approximately 15% stake in the company, Congressman Robert Pittenger (R-NC) wrote in the Wall Street Journal that, "If [the acquisition was to be] approved, the Chinese government would gain significant access to, and information on, financial markets and specific international consumer money flows."[14]

- Lawmakers also expressed concern over the proximity of MoneyGram's headquarters and money transfer agents to U.S. military bases and its use by many service members to send remittances home. Sen. Jerry Moran (R-KN) said in an interview that, "Part of [lawmakers'] concern is that [MoneyGram] provides services to military men and women and their families, and access to that kind of data creates potential for information you do not want others to have."[15]

In a separate incident, Euronet Worldwide entered into a bidding war with Ant Group in March 2017 over MoneyGram, positioning itself as the safer alternative with respect to national security and data privacy concerns, but was outbid. Following the collapse of Ant Group's MoneyGram acquisition, Euronet issued a statement:

> "We will continue to advocate that, in view of its ownership and its practices, Ant Financial does not meet the standards to assume the responsibilities of a U.S. money transmitter. This includes demonstrating an ability to protect sensitive personal information on U.S. citizens and military personnel as well as the need to uphold and participate in U.S. Federal and State efforts related to regulating anti-terrorism financing and money laundering."[16]

[13] https://www.sec.gov/Archives/edgar/data/1273931/000119312518000668/d517771d8k.htm
[14] https://www.wsj.com/articles/check-chinas-financial-investments-in-the-u-s-1487700633
[15] 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/
[16] https://ir.euronetworldwide.com/index.php/news-releases/news-release-details/euronet-worldwide-comments-moneygram-and-ant-financial-cfius

2. Role in Mass Detention and Surveillance in the Xinjiang Uyghur Autonomous Region (XUAR)

Ant Group and Alibaba are both investors in Megvii Technology, an artificial intelligence (AI) startup that specializes in facial recognition technology.[17] Both companies are also customers of Megvii: Ant Group has used the company's Face++ system to power restaurant payment concepts and Alibaba uses Face++ to analyze CCTV networks for incident reporting through its City Brain platform.[18] In addition to its various commercial applications, Face++ was identified in May 2019 as a component of the Integrated Joint Operations Platform (IJOP) used by police and other authorities in Xinjiang for mass surveillance purposes.

The human rights organization that had initially flagged the use of Face++ in IJOP, however, issued a correction one month later stating that Megvii did not appear to have collaborated on IJOP and its Face++ code in the app appeared "inoperable."[19] Nevertheless, Megvii was sanctioned by the U.S. government and added to the Entity List maintained by 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, mass arbitrary detention, and high-technology surveillance in the XUAR."[20]

3. Military Dual-Use Potential

The Chinese military-industrial complex is rapidly modernizing through the integration of military and civilian technology, particularly in the areas of artificial intelligence (AI) and big data. Alibaba has been identified by the U.S. government as a leading participant in this program, known as military-civil fusion.[21] China, like certain other countries, is engaged in big data research for national defense purposes, with a focus on building advanced data aggregation and processing capabilities to advance, for example, military intelligence-gathering and analysis.

[17] https://techcrunch.com/2019/08/26/megvii-the-chinese-startup-unicorn-known-for-facial-recognition-tech-files-to-go-public-in-hong-kong/
[18] https://bernardmarr.com/default.asp?contentID=1883
[19] https://www.scmp.com/tech/start-ups/article/3013229/ai-unicorn-megvii-not-behind-app-used-surveillance-xinjiang-says
[20] https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list
[21] https://cn.wsj.com/articles/%E4%B8%AD%E5%9B%BD%E5%80%9F%E6%B0%91%E8%90%A5%%BC%81%E4%B8%9A%E6%8F%90%E5%8D%87%E5%86%9B%E5%8A%9B%E5%BC%95%E8%B5%B7%E7%BE%8E%E5%9B%BD%E8%AD%A6%E6%83%95-11569460807

- In January 2019, the regional representative for Alibaba reportedly met with the Municipal Development and Reform Commission of Xi'an province to discuss the potential for cooperating on military-civil fusion opportunities alongside Xi'an-based information technology companies.[22]

- During the PLA Academy of Military Science's first annual military big data forum in July 2018, where military, academic, and corporate leaders discussed ways to transition the benefits and technologies of e-commerce to national defense, an Alibaba Cloud Computing executive made a presentation on the role of big data in urban governance through services such as monitoring and early warning, emergency command, intelligent decision-making, and operational linkage.[23]

4. Participation in Social Credit System Construction

One of Ant Group's subsidiaries, Zhima Credit Management (Sesame Credit), is among the eight private companies that received provisional permissions from the People's Bank of China (PBOC) in January 2015 to facilitate the development of credit scores using their existing access to data. The private credit scoring programs were intended to supplement the state-run personal credit database. Using large-scale data collection and analysis, this personal credit database reportedly assigns scores to its citizens based not just on their economic reputations, but also on their social track records.[24] Citizens then receive benefits and rewards (or punishments) throughout their daily lives based on how they have scored.[25]

- In August 2016, Ant Financial signed a memorandum of cooperation with China's National Development and Reform Commission (NDRC) to implement "joint rewards and punishments." According to CEO Jing Xiandong, Zhima Credit would, under the banner of Ant Financial, "share information collected on trustworthiness and untrustworthiness with the State Credit Information-Sharing Platform in a timely manner and in accordance with the relevant laws, regulations, and supervisory requirements."[26]

[22] https://chuansongme.com/n/2772062852631; https://kuaibao.qq.com/s/20190117A14NK300?refer=spider
[23] http://www.d1net.com/bigdata/news/530236.html
[24] https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590
[25] https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4
[26] https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-22210.pdf

- As of July 2017, Zhima Credit was the most popular of the eight government approved companies operating in this space and had successfully expanded its services beyond credit provision to general trustworthiness using financial data from Alibaba and Ant Financial to evaluate user identities, online activity, and social networks.[27] Of the eight companies, Zhima Credit and Tencent Credit held the largest amounts of customer data at their disposal.[28]

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 them shareholders in a new unified personal credit information platform known as Baihang Credit Scoring.[29] Baihang Credit is now the only Chinese entity with permissions to conduct both personal and enterprise credit rating operations.

Baihang Credit stated in July 2020 that it had signed data integration sharing agreements with nearly 1,000 organizations.[30] It also claims to have received "very considerable support [from shareholders] with regard to the five areas of systems development, product R&D, technical strength (personnel), market expansion, and the sharing of lending information." It is unclear whether Ant Group and Zhima Credit are among these shareholders, as, in September 2019, it was reported that Ant Group had declined to provide Baihang Credit with access to Zhima Credit's vast trove of data (including its data on individuals from various Alibaba e-commerce sites and finance products including Taobao, Tianmao, and Alipay).[31, 32] Ant Group's reluctance at the time, however, was attributed to competitive concerns it had over the value of its data, not necessarily to data privacy issues.

[27] https://www.piie.com/system/files/documents/pb18-1.pdf
[28] https://www.business-humanrights.org/en/latest-news/china-alibaba-and-tencent-refuse-to-share-loans-data-with-government-backed-credit-scoring-company/
[29] http://www.xinhuanet.com/english/2018-02/22/c_136991905.htm; https://www.caixinglobal.com/2018-05-28/launch-of-unified-platform-boots-private-firms-from-personal-credit-business-101258187.html
[30] http://www.chinabankingnews.com/2020/07/23/baihang-credit-amasses-data-on-130-million-borrowers-in-china
[31] https://www.whatsonweibo.com/baihang-and-the-eight-personal-credit-programmes-a-credit-leap-forward/; https://www.ft.com/content/93451b98-da12-11e9-8f9b-77216ebe1f17
[32] http://www.chinabankingnews.com/2019/09/26/baihang-credit-enters-cooperative-discussions-with-alibaba-and-tencent/

5. Data Collection and Privacy Concerns

The fintech sector inherently faces heightened cybersecurity risk, with personal and financial user data (connected to banks and other financial institutions) subject to theft or breaches of privacy. Having one company act as the sole arbiter of payments creates easier access for ill-intentioned actors to breach and access sensitive individual and institutional data, including but not limited to data on finances, social networks, and location. These concerns are exacerbated by the reality that even "private" Chinese companies are beholden to Chinese government interests, and that the government's data appropriation powers are memorialized in national intelligence (i.e., Article 7 of the National Intelligence Law) and security laws and regulations.

Ant Group's poor record of privacy has been recognized by even China's cyber watchdog, the Cyberspace Administration of China (CAC), which released a statement in January 2018 accusing the company of failing to meet national security standards for personal information. The CAC statement was released in response to accusations of user privacy violations after AliPay users found themselves automatically enrolled in a credit scoring system operated by Ant Group subsidiary Zhima Credit, which received access to users' personal financial data to share with partners.[33]

At the beginning of the COVID-19 epidemic in China, Ant Group introduced a system known as the Alipay Health Code, accessible through the Alipay mobile app, intended to help enforce government quarantine guidelines through color-coded indicators of health status. The system was reportedly developed in partnership with law enforcement authorities and includes programming that sends the user's location information and other identifiers to the police, once certain app permissions are granted. This data-sharing arrangement has been characterized as an unusually direct example of private-public collaboration and setting a precedent for mass surveillance in China.[34]

Additionally, Alipay often uses facial recognition technology in its payment products and systems, which has raised long-standing concerns over privacy and data, including with regard to potential fraud, account hacking via impersonation, data privacy and the possibility of personal data being passed on to the CCP. Other foreign governments have also expressed these misgivings. Earlier this month India banned Alipay and 117 other Chinese-owned or

[33] https://www.caixinglobal.com/2018-01-11/ant-financial-to-review-privacy-policy-after-receiving-slap-on-wrist-101196761.html
[34] https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

linked apps due to these data collection and privacy concerns.[35] A statement by India's Ministry of Electronics & IT stated with regard to the mass ban of apps,

> "The compilation of these data, its mining and profiling by elements hostile to national security and defence of India, which ultimately impinges upon the sovereignty and integrity of India, is a matter of very deep and immediate concern which requires emergency measures."[36]

6. Government Ties and Influence

Ant Group would likely not have attained its current state of prominence without the backing of the Chinese government, despite being an ostensibly private enterprise, due to the government's immense influence on the market. The Chinese government, for the most part, dictates the rules of commercial success: companies that it wants to succeed generally succeed, and companies that it wants to fail tend to fail.

When the State Administration for Industry and Commerce released a document critical of Alibaba in 2015, the company lost $37 billion in market value in just four days.[37] Despite founder Jack Ma's insistence that the company will "only fall in love with the government and never get married," the success of Alibaba and its subsidiaries represent evidence that they recognize and comply with these rules. More revealing is Ma's comment during a 2017 interview, that, "As long as the country needs it, we are ready to dedicate Alipay to the country at any time."[38]

In a move that affirms the Chinese government's oversight of even companies that are not state-owned, Hangzhou's municipal government introduced a new initiative in its New Manufacturing Plan released in September 2019: deploying government officials to 100 key enterprises, including Alibaba, to serve as government affairs representatives. The representatives will, according to a statement by Alibaba on the matter, "function as a bridge

[35] https://www.scmp.com/abacus/tech/article/3029480/facial-recognition-payments-are-privacy-risk-says-china-central-bank; https://www.scmp.com/abacus/tech/article/3029480/facial-recognition-payments-are-privacy-risk-says-china-central-bank
[36] https://pib.gov.in/PressReleasePage.aspx?PRID=1650669
[37] https://www.wenxuecity.com/news/2019/09/11/8667303.html; https://www.reuters.com/article/us-alibaba-group-saic/alibaba-meets-with-china-regulator-controversial-report-retracted-idUSKBN0L31S020150131
[38] https://v.qq.com/x/page/f05063v2xbg.html

between the government and the private sector," and will be tasked to help with project implementation, policy interpretation, and communications.[39]

In response to public concern about the potential for government control and interference that might result from this Hangzhou initiative, Alibaba issued a statement:

> "We understand this initiative... aims to foster a better business environment in support of Hangzhou-based enterprises. The government representative will function as a bridge to the private sector and will not interfere with the company's operations."[40]

The Chinese government has also mandated "Party building" in the private sector – which is manifested in the creation of CCP cells and/or working groups within the senior management structures of companies – and the fintech industry is no different.[41] According to the Beijing Internet Association, which is governed by the Beijing Municipal Committee of the CCP's Cyber Security and Informatization Committee and tasked with implementing the Party and government's Internet policies and regulations, the top 100 Internet companies in the country have all established Party organizations.[42] Alibaba's Party committee has reportedly stood up a sizeable team for the purposes of research and development, management, and marketing operations.[43]

Externally, Alibaba and Ant Group maintain strong ties to the municipal government of Hangzhou and play a role in key projects. Various comments by government officials affirm the elevated significance of the company's network to the city's growth and development.

- Dai Jianping, a Standing Committee member of the CCP Hangzhou Municipal Committee responsible for supervising the city's financial institutions, said during a visit to Ant Group in May 2020 that Hangzhou should "fully support the development of key

[39] https://www.reuters.com/article/us-alibaba-china-party/china-to-send-state-officials-to-100-private-firms-including-alibaba-idUSKBN1W80DQ
[40] https://fr.reuters.com/article/companyNews/idUKKBN1W80DL
[41] Alibaba Group is publicly traded on the NYSE but considered a listed "private" company in China, in contrast with "public" state-owned enterprises. http://www.globaltimes.cn/content/1064500.shtml
[42] http://news.sina.com.cn/c/nd/2018-03-26/doc-ifysrnnk1362359.shtml
[43] http://szjggw.hangzhou.gov.cn/art/2019/11/11/art_1079299_40072871.html; http://szjggw.hangzhou.gov.cn/module/download/downfile.jsp?classid=0&filename=894adeb1167240e0bef6fd2d4aa91a03.pdf

companies such as Ant Group [and] strive to achieve the mutual promotion of corporate innovation and government services."[44]

- One month later, Alibaba signed an agreement with the Hangzhou government during an annual joint meeting to accelerate the construction of China's first digital governance city and to launch several projects including the second phase of the Zhejiang cloud computing center, the second phase of the Ant Group headquarters, and the new Cainiao Supply Chain Financial Industrial Park.[45]

- Alibaba and Ant Group have also signed strategic cooperation agreements with other government entities, including the provincial government of Chengdu and the government of the Guangxi autonomous region, both in ceremonies attended by local Party committees.[46]

7. Vulnerability to Escalating Geopolitical Tensions

India's technology sector has become a key battleground in its continually escalating geopolitical rivalry with China. In January 2020, Indian food delivery startup Zomato announced that Ant Group had committed to investing $150 million in the company. In late July, a Zomato investor noted that "Ant Group had yet to deliver two-thirds of the capital," which Ant claims is due to regulatory changes in India that require foreign direct investment from any country sharing a land border with India to undergo a government approval process.[47]

A military standoff on the border resulted in the deaths of 20 Indian soldiers in June, 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."[48] In response, at the

[44] http://szjggw.hangzhou.gov.cn/art/2019/11/11/art_1079299_40072871.html; http://szjggw.hangzhou.gov.cn/module/download/downfile.jsp?classid=0&filename=894adeb1167240e0bef6fd2d4aa91a03.pdf
[45] http://www.hzgh.org/newsview75848.htm
[46] https://www.sc.gov.cn/10462/10605/13622/13623/2017/2/27/10415275.shtml; http://finance.jrj.com.cn/2020/08/19114530537206.shtml
[47] https://foreignpolicy.com/2020/04/28/india-china-fdi-restrictions-coronavirus/; https://techcrunch.com/2020/09/02/indias-zomato-raises-62-million-from-temasek/
[48] https://www.ft.com/content/b1df5dfd-36c4-49e6-bc56-506bf3ca3444

end of August, it was reported that Alibaba would halt all new investment into any Indian startups for at least six months due to escalating border tensions.[49]

- On September 2, 2020 the Indian Ministry of Electronics & Information Technology announced its decision to block AliPay, TaoBao, and another 116 China-based or -linked apps, citing complaints that the apps are "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India."[50] Though the Ministry's announcement does not name China specifically, this expansion has been linked to the recent killing of an Indian soldier by a Chinese land mine along the countries' disputed border in Kashmir.[51]

- Nepal also issued a ban on AliPay and WeChat Pay in May 2019, claiming that payments through the apps were illegal as neither app was registered with Nepal's regulatory body. A spokesperson for the Nepal Rastra Bank alleged that, although AliPay payments used Nepal's internet connectivity, the transactions were in fact made in China, and thus not taxable or reflected in Nepal's national accounts.[52]

The United States has likewise been ratcheting up pressure on Chinese apps, on the grounds of data privacy and national security concerns. In August 2020, the Trump administration issued an executive order banning two major Chinese apps, WeChat and Tiktok.[53] The escalation of tensions in this domain between the United States and China puts Alipay and Ant Financial – as well as affiliate Alibaba – at risk of financial repercussions stemming from potential U.S. government action against these enterprises, which could harm U.S. and other investors.

[49] https://techcrunch.com/2020/08/26/chinas-alibaba-wont-invest-in-indian-startups-for-at-least-six-months-report-says/
[50] https://pib.gov.in/PressReleasePage.aspx?PRID=1650669
[51] https://www.nytimes.com/2020/09/02/world/asia/india-bans-china-apps.html#:~:text=the%20main%20story-,India%20Bans%20118%20Chinese%20Apps%20as%20Indian%20Soldier%20Is%20Killed,amid%20a%20tense%20border%20standoff.
[52] https://www.reuters.com/article/us-china-nepal-digitalpayments/nepal-says-bans-wechat-pay-alipay-idUSKCN1SS19N
[53] https://www.brookings.edu/blog/up-front/2020/08/07/why-is-the-trump-administration-banning-tiktok-and-wechat/

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.