FANGDA PARTNERS
方達津師事務所

China's New Regulation on Network Data Security Management – What Companies Should Know

October 3, 2024

NEWSLETTER

CONTACT

Kate Yin
Partner, Fangda Partners
kate.yin@fangdalaw.com

Gil Zhang
Partner, Fangda Partners
gil.zhang@fangdalaw.com

Sherman Deng
Partner, Fangda Partners
sherman.deng@fangdalaw.com

Li Huihui
Partner, Fangda Partners
huihui.li@fangdalaw.com

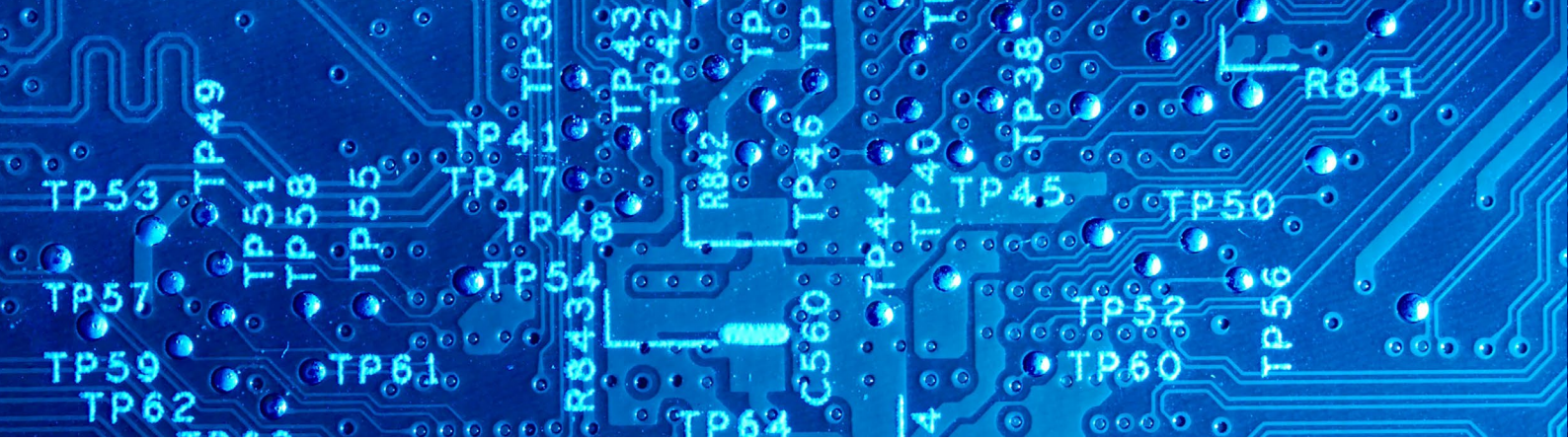
The "Regulation on Network Data Security Management" (the "**Regulation**", in Chinese 网络数据安全管理条例) was approved by the State Council and released on September 30, 2024, and will come into effect on January 1, 2025. This Regulation provides detailed operational guidelines for the implementation of China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL), collectively known as the "Three Key Laws." The Regulation requires various supervisory authorities to coordinate and align different data compliance mechanisms and requirements under different inspection items, striving to strengthen the connection and mutual recognition of inspection results within the overlapped scopes.

The Regulation took almost three years to finalize, from the first draft published for public comment on November 14, 2021 (the "**2021 Draft**"), to its release on September 30, 2024. Chinese regulators reconciled the Regulation with the Three Key Laws and other measures such as cross-border data transfer based on its experience in law enforcement in the past three years. Given its broad scope, this newsletter focuses on key topics relevant to foreign businesses: (i) cross-border data transfer ("**CBDT**"), (ii) important data, (iii) personal information protection, (iv) penalties; (v) large network platforms and their compliance obligations; and (vi) government access to data.

1. Cross-Border Data Transfer

Representative for Foreign Data Handlers

Foreign data handlers (similar to a data controller under GDPR) processing personal information of Chinese citizens from outside China (e.g., a foreign website targeting Chinese residents) must



appoint a representative within China. This representative must be reported to the local branch of the Cyberspace Administration of China (CAC) at the municipal level. The representative ensures compliance with Chinese data protection laws and serves as the point of contact for regulatory authorities. Now that the Regulation reiterates the appointment of local representative, CAC's detailed rules on the appointment and the filing guidance may come soon.

Transfer Mechanism

The Regulation recaps the existing mechanisms for lawful cross-border data transfers and signals the finalization of rules around the threshold and different mechanisms, including security assessment, certification, standard contract filing and data transfers for special scenarios such as those necessary for contract performance, cross-border human resource management, or to protect individuals' life or property in emergencies.

The Regulation does not specify volume thresholds for these mechanisms, allowing flexibility for the CAC and authorities in Pilot Free Trade Zones (FTZs) to relax cross-border data transfer rules. Efforts to this effect have already been seen in the FTZs of Beijing, Shanghai, and Tianjin.

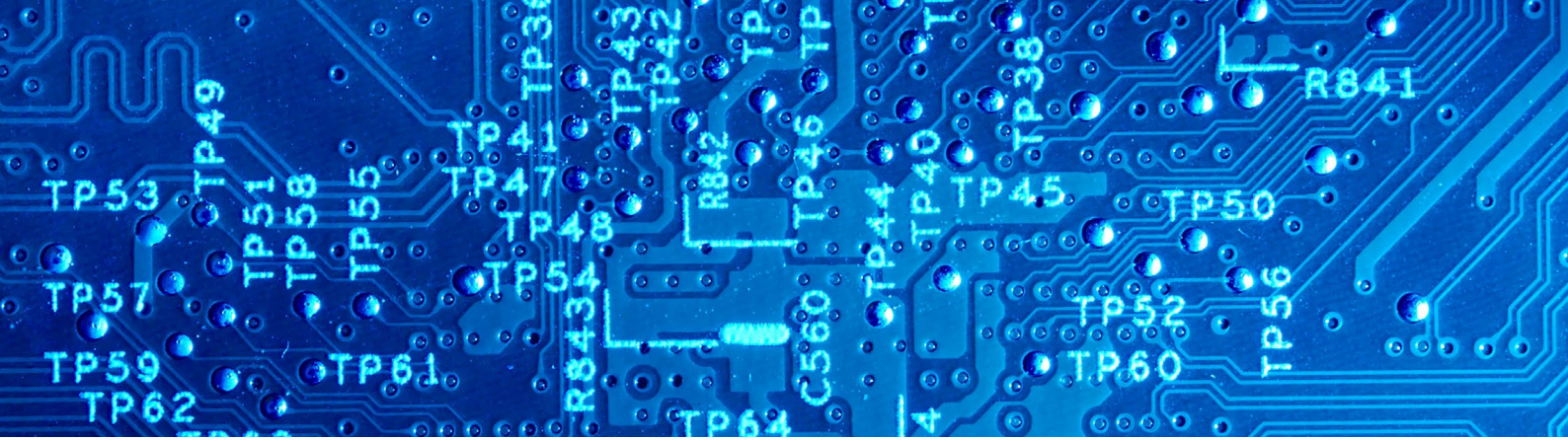
Data Localization

The Regulation emphasizes data localization, requiring certain types of data, particularly important data and large volumes of personal information, to be stored within China. Exceptions are subject to stringent security assessments and approvals. Notably, the final version of the Regulation removed the ban on foreign government agencies accessing data stored in China, a position already solidified under the DSL and PIPL. Additionally, the CBDT security gateway, strict ban on VPNs and rerouting traffic to foreign networks mentioned in the 2021 Draft was also removed.

2. Important Data

Scope and Definition

Important data is defined as data that, if tampered with, destroyed, leaked, or illegally obtained or used, could directly harm national security, economic operations, social stability, public health, and safety. Processing personal information of 10 million individuals or more appears to be classified as important data as well. Catalogues of important data can be found in national standards and "negative lists" promulgated by FTZs, though these catalogues currently lack detailed operational guidelines.



Affirmative Obligation to Identify and Report

Once Chinese regulators publish or notify a specific company or sector on the catalogue or scope of important data, data handlers must identify and report important data to relevant authorities, conduct regular risk assessments, and submit reports on the handling and protection of important data. Non-compliance can result in severe penalties, including fines and business restrictions as mentioned below.

Important Data Sharing

- **Cross-Border Sharing:** Heavily regulated, requiring security assessments and approvals before transferring important data abroad. If data is not officially categorized as important by government notice or public rule, data handlers are not obligated to apply for security assessments for its cross-border transfer.

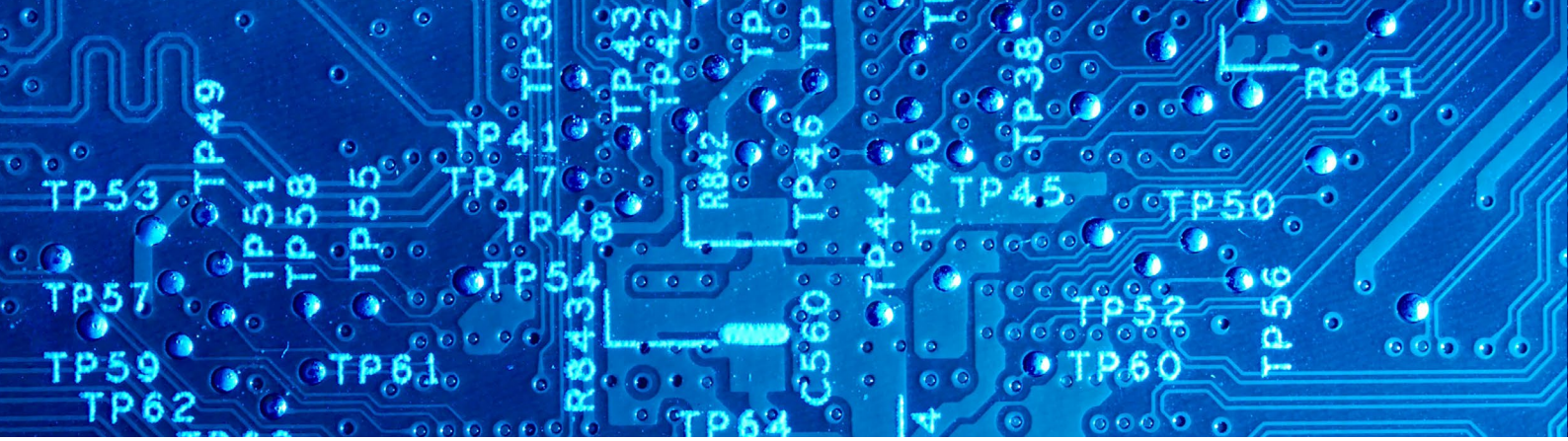
- **Domestic Sharing:** Must be conducted under strict contractual agreements outlining the purpose, method, scope, and security obligations of the receiving party. Sharing must pass a test of legality, legitimacy, and necessity, meaning it is not allowed if there is no lawful basis or if there is an alternative method to achieve the processing purpose without sharing the important data.

Based on our experience handling important data related matters, we would recommend foreign companies adopt a "top-down" approach around "access, intent and knowledge" to minimize exposure to important data, document intentions in contracts and policies, and build employee awareness. Additionally, a "bottom-up" approach to classify, identify, and inventory important data as required by the Regulation is recommended. Companies must carefully consider whether to report identified important data to authorities.

3. Personal Information (PI) Protection

PI Protection Audit

Data handlers are required to conduct regular privacy audits to ensure compliance with data protection laws and regulations. These audits assess the effectiveness of data protection measures and identify potential vulnerabilities. Professional institutions may be engaged to perform these audits, providing an independent evaluation of the data handler's compliance status. The CAC is working on draft rules and standards that will require data handlers processing large volumes of data to conduct annual PI Protection Audits. Based on our experience, these projects are resource-intensive and time-consuming, so foreign companies should plan ahead. The Regulation specifically requires Chinese regulators to coordinate and provide interoperability of audit or risk assessment on companies in different contexts, aiming to reduce the burden of companies having to repeat the compliance efforts for different regulators.



Data Subject Rights (DSR)

Individuals have the right to access, correct, delete, and restrict the processing of their personal information. Data handlers must provide convenient methods for individuals to exercise these rights and respond to requests promptly. This empowers individuals to have greater control over their personal data and ensures transparency in data processing activities. However, DSR is not absolute; the Regulation permits data handlers to set reasonable conditions and restrictions on DSR. We have observed a trend where data subjects in potential legal disputes use DSR to gather evidence before filing lawsuits and may complain to the CAC if their requests are not met. We recommend that foreign companies clearly outline the conditions for exercising DSR, retention periods, and channels for exercising DSR to properly respond to these requests and potential enforcement actions.

Data Breach

In the event of a data breach, data handlers must immediately activate their incident response plans to mitigate the impact and eliminate security risks. They are required to report the breach to relevant authorities. If the breach causes harm to individuals, the data handler must notify affected individuals and relevant authorities, detailing the nature of the breach, potential consequences, and measures taken to address it. Individual notification is "harm-based," meaning it is not required if, after reasonable investigation, the data handler determines there is no reasonable likelihood of harm to individuals. However, authorities may disagree with this determination and mandate notification. Based on our experience, the requirements for individual notification vary across regions and industries, and the format of notifications can differ significantly.

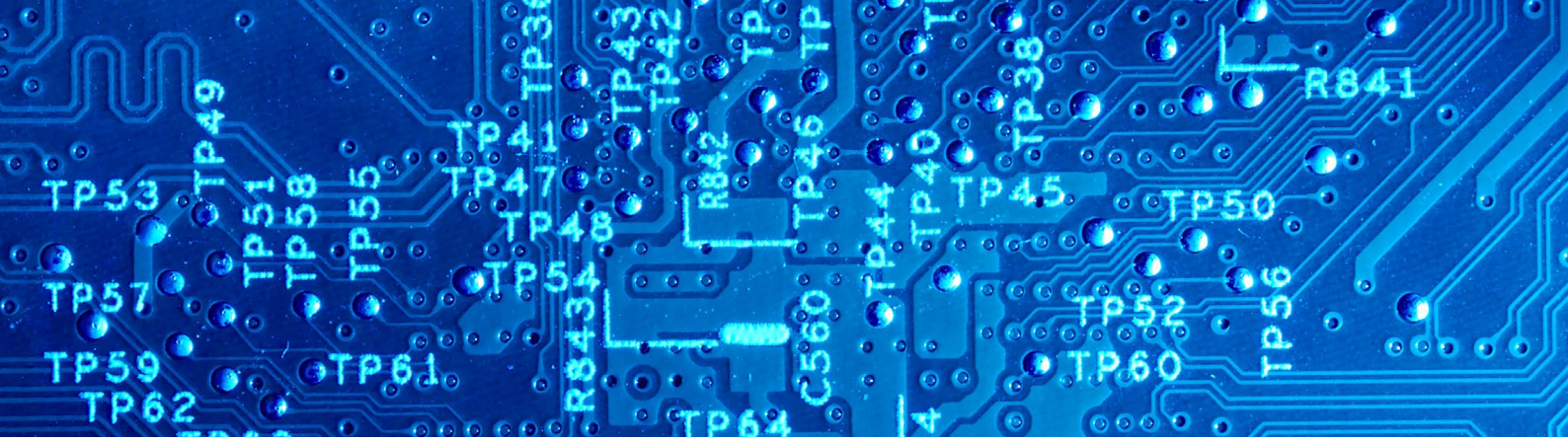
4. Penalty for Violation

Violating CBDT Regulations

Under the 2021 Draft, violations of cross-border data transfer regulations could result in significant penalties, including fines ranging from RMB 1 million to RMB 10 million, suspension of business operations, or revocation of business licenses. Responsible personnel could also be fined. However, this provision was removed from the final version. The default penalty now aligns with the PIPL, which imposes fines of up to RMB 50 million or 5% of annual turnover.

Violating Important Data Protection

Failure to protect important data, including failure to identify and report it, can lead to severe consequences under the Regulation. Penalties include fines of up to RMB 2 million, suspension of business operations, and



revocation of business licenses. Additionally, responsible personnel may face fines and other disciplinary actions. These stringent penalties underscore the critical importance of safeguarding important data.

Violating PI Protection Regulations

The Regulation specifies penalties for certain privacy violations, including failure to perform third-party risk management (TPRM) obligations (e.g., entering into Data Processing Agreements), failure to obtain proper consent from individuals for data processing, and failure to allow individuals to opt out of automated decision-making. Data handlers may be fined up to RMB 1 million for these violations. Responsible personnel may also be held accountable, facing fines and other sanctions.

5. Large Network Platforms

The Regulation defined "large network platforms" as those with over 50 million registered users or more than 10 million monthly active users with characteristics of (a) complex business types and (b) network data processing activities that significantly impact national security, economic operations, and public welfare. These two characteristics may require further clarification from regulators.

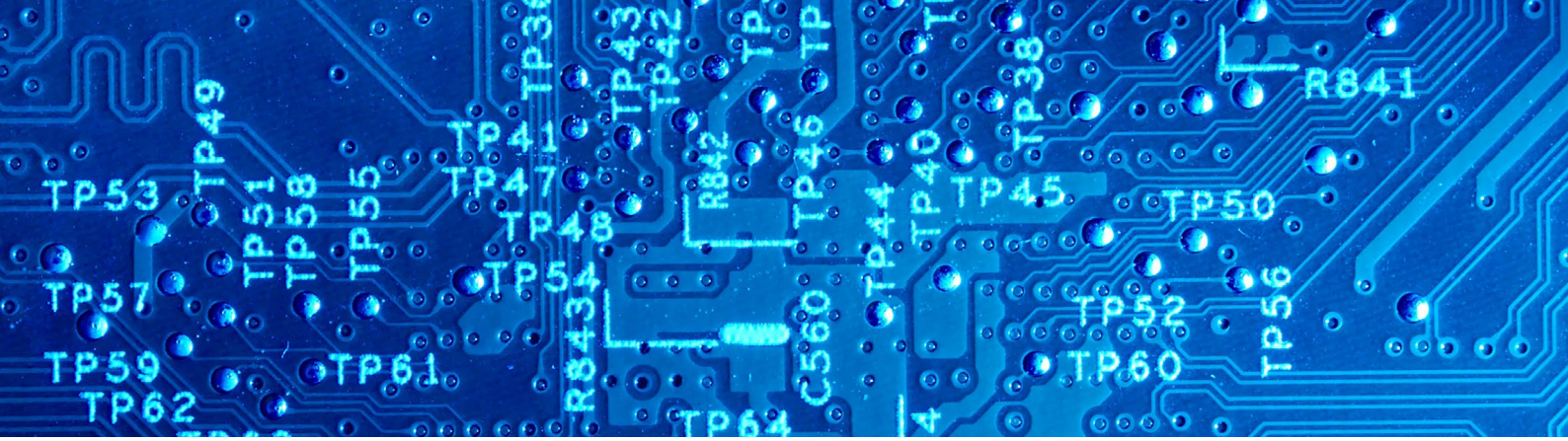
Compliance and obligations of large network platforms on top of the other data protection and cyber security requirements are summarized as follows:

Social Responsibility Report

Additionally, Article 44 of the regulations draws from Article 58 of the Personal Information Protection Law, mandating large network platforms to publish an annual social responsibility report on personal information protection. This report must detail measures and effectiveness of personal information protection, the handling of DSR's, and the performance of duties by personal information protection oversight bodies, among other aspects.

Watchdog Obligations Regarding Third-Party Merchants

Large network platforms are required to perform "watchdog" duties to help regulators oversee third-party merchants' data security practice. Manufacturers of smart devices with pre-installed applications will have the same obligations. In particular, online content distributers, such as mobile app store operators, will have the obligations to test the app's before distribution and take measures such as warnings, suspension, or termination of distribution for non-compliant apps.



Other Obligations

Large network platforms are also required to provide opt-outs for automated decision-making, cooperate with the government on the roll-out of unified digital ID, comply with CBDT, refrain from unfair and deceptive acts and practices such as misleading, fraudulent, or coercive data processing, unjustified restrictions on user data access, unreasonable differential treatment of users, and other prohibited activities by law.

6. Government Data Access Restrictions

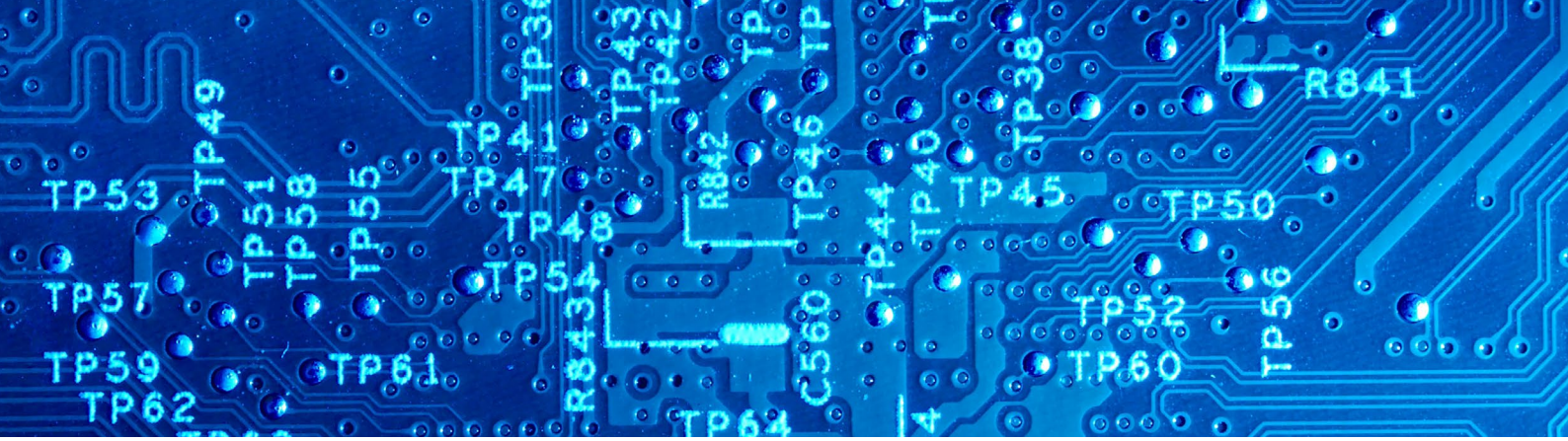
In response to some international disputes regarding government data access, Article 51 of the Regulation reaffirms the corresponding rules, stating that relevant authorities shall not access or collect business information unrelated to network data security during the supervision and inspection of network data security. The information obtained can only be used for the needs of maintaining network data security and shall not be used for other purposes.

Regarding the issue of fragmented law enforcements that has emerged in the past few years, Article 52 of the Regulation also emphasizes that relevant authorities should strengthen coordination and cooperation, and improve information communication when conducting supervision and inspection of network data security. They should reasonably determine the frequency and methods of inspection to avoid unnecessary and overlapping inspections. There should be better coordination in personal information protection compliance audits, risk assessments of important data, and security assessments of important data exports to prevent redundant assessments and audits.

Conclusion

This Regulation represents the maturation of the Three Key Laws. We anticipate increased enforcement and on-site inspections now that the Regulation provides more detailed operational guidelines and tailored penalties for different violations. Multinational companies doing business in China should prioritize the control points mentioned in the Regulation.

- For CBDT, we recommend complying with the applicable transfer mechanisms and completing the necessary procedures.
- For important data, we suggest building a defense system around "access, intent, and knowledge" and working on important data classification.
- For PI protection, we recommend conducting a PI protection health check and planning for regular PI protection audits.



Beijing

27/F, North Tower
Beijing Kerry Centre
1 Guanghua Road
Chaoyang District
Beijing 100020, China

Tel: +86 10 5769 5600
Fax: +86 10 5769 5788

Guangzhou

66/F, Guangzhou CTF
Finance Centre
6 Zhujiang East Road
Zhujiang New Town
Guangzhou 510623, China

Tel: +86 20 3225 3888
Fax: +86 20 3225 3899

Hong Kong

26/F, One Exchange Square
8 Connaught Place, Central
Hong Kong

Tel: +852 3976 8888
Fax: +852 2110 4285

Nanjing

38/F, Asia Pacific Business Building
2 Hanzhong Road
Gulou District
Nanjing 210005, China

Tel: +86 25 8690 9999
Fax: +86 25 8690 9099

Shanghai

24/F, HKRI Centre Two,
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041, China

Tel: +86 21 2208 1166
Fax: +86 21 5298 5599

Shenzhen

9/F, Tower One, Kerry Plaza
1 Zhong Xin Si Road
Futian District
Shenzhen 518048, China

Tel: +86 755 8159 3999
Fax: +86 755 8159 3900

Singapore

1 Raffles Place #55-00
One Raffles Place Tower 1
Singapore 048616

Tel: +65 6859 6789
Fax: +65 6358 2345