HANKUN
汉坤律师事务所
Han Kun Law Offices

Han Kun Newsletter

Issue 212 (12th edition of 2024)

Legal Updates

1. NFRA Data Security Measures – Implications for Foreign Funded Banks
2. CTA Update: BOI Reporting Obligation is Once Again Suspended
3. Strengthening Oversight of Imported Drugs: Key Takeaways into New Regulations on Domestic Responsible Entities
4. CTA Update: BOI Reporting Requirements Reinstated
5. Han Kun Legal Updates on the Corporate Transparency Act (CTA)

1. NFRA Data Security Measures – Implications for Foreign Funded Banks

Authors: Ting ZHENG | Raymond YAN | Eryin YING | Lin ZHU | Shirley LIANG | Hattie ZHANG

The National Financial Regulatory Administration ("**NFRA**") released the *Measures for Data Security Management of Banking and Insurance Institutions (《银行保险机构数据安全管理办法》)*("**Data Security Measures**") on 27 December 2024, which came into effect immediately upon promulgation. Prior to that, NFRA circulated the first draft among banks on 5 September 2023 and the second draft to solicit public comments on 22 March 2024 ("**Draft Measures**"). The Data Security Measures substantially stay the same as the Draft Measures, with only minor wording changes and non-substantial additions.

We set out below the key requirements under the Data Security Measures and potential implications for foreign funded banks (including subsidiary banks and where applicable, foreign bank branches) ("**Banks**" or a "**Bank**") in China.

No.	Key requirements	Implications and actions
General		
1	NFRA and its local offices are in charge of data security in the banking sector and will supervise and inspect the performance of data security duties by commercial banks.	This echoes Art.6 of the *Data Security Law* (《数据安全法》) ("**DSL**").
2	A Bank shall set up a data security governance system accommodated to its business development and it shall contain the following key aspects: ■ data life cycle protection covering all application scenarios; ■ data security risk assessment; and ■ data security risk monitoring, alerts and handling.	This largely follows the general principles under the *Guidelines for the Data Governance of Banking Financial Institutions (《银行业金融机构数据治理指引》)* ("**Banking Data Governance Guidelines**") and provides additional implementing requirements as further described below.
Data security governance system		
3	The party committee and the board of directors shall take the ultimate responsibility for data security. The responsible person (chairman of board or the president of a foreign bank branch) of a Bank shall be the primary responsible person. Other senior officers who are designated to lead data security tasks[1] shall be directly responsible persons.	This requirement is originally from and similar as the Banking Data Governance Guidelines. Furthermore, the Data Security Measures provide that the party committee shall be ultimately responsible for data security, but we

[1] Note: in Article 10 of the Data Security Measures, the term "leaders (领导)" in charge of data security is replaced with the term "senior officers (高级管理人员)", which has provided more clarity.

No.	Key requirements	Implications and actions
General		
		understand this should not apply to the Banks which don't have the party committee.
4	A data security centralized management department (数据安全归口管理部门) shall be designated to perform the new duties in terms of data classification and grading, security assessment, emergency handling and risk monitoring, training, and management of internal or external data sharing and third-party data providers.	The Banking Data Governance Guidelines have required a Bank to set up a centralized management department, but the Data Security Measures provide certain new duties as stated in the left column. Additionally, the Data Security Measures do not require the centralized management department to be an independent and dedicated department. A Bank reserves the flexibility to determine a centralized management department based on its actual internal management needs, but data-dedicated positions are still required.
5	Each of business department, risk management department, compliance and audit department, and IT department shall play certain duties for data security.	This is not new. The data security governance structure and each department's role have been provided in further details in existing national standards (e.g., the *Financial Data Security - Security Specification of Data Life Cycle* (*《金融数据安全 数据生命周期安全规范》*) ("**Financial Data Life Cycle Security Specification**").
Data classification and grading		
6	Data shall be classified into client data, business data, operation and management data, system operation and security management data, etc.	This is a new classification system, but existing national standards (e.g., the *Financial Data Security - Guidelines for Data Security Classification* (*《金融数据安全 数据安全分级指南》*) ("**Financial Data Classification Guidelines**") have provided similar classifications.
7	Data grading includes core data, important data and general data. General data is further divided into sensitive data and other general data.	This grading system is generally consistent with the grading system provided in Article 21 of the DSL, but is slightly different as it defines general

No.	Key requirements	Implications and actions
General		
		data and sub-divides general data into sensitive data and other general data. This is also slightly different from the 1-5 grading methodology in existing national standards (e.g., the Financial Data Classification Guidelines). We understand NFRA will issue detailed data grading rules. Please also note that the People's Bank of China ("**PBOC**") has released the *Administrative Measures for Data Security in PBOC's Business Area (Draft for Comment)* (《*中国人民银行业务领域数据安全管理办法(征求意见稿)*》) to regulate the data security relating to the businesses under PBOC's jurisdiction, such as interbank trading business, payment and clearing business, KYC, etc. Further clarity may be required as to how the two grading systems should be applied to a Bank. PBOC has clarified that it will actively support other competent authorities to perform their data security administrations, and will agree on the regulatory cooperation mechanism where necessary.
8	A Bank shall conduct dynamic adjustments on data grading with changes in data attributes, level of importance and potential damages.	This is a new requirement, but existing national standards (e.g., the Financial Data Classification Guidelines) have provided a similar requirement.
Data security management		
9	The Data Security Measures borrows many full-life-cycle management measures for personal information under the *Personal Information Protection Law* (《*个人信息保护法*》) ("**PIPL**") and apply them to all data (including corporate data). The key measures are detailed below in this section. Notably, the Data Security Measures provide that the collection, utilization, sharing, and joint processing of data (including corporate data) shall all be based on the principle of necessity.	The Data Security Measures expand the application of many requirements for the processing of personal information to the processing of all data (including corporate data). Banks should take the key measures in this section below towards its processing of all data (including corporate data).

No.	Key requirements	Implications and actions
	General	
10	Prior data security assessment is required for: ■ processing of sensitive data, important data and core data; and ■ entrusted processing, joint processing, transfer, disclosure or sharing of data.	The application of data security assessment is expanded beyond processing of personal information ("**PI**") and important data required under PIPL and DSL. Banks need to ensure their data security assessment procedures apply to all required scenarios as stated in the left column.
11	Procurement of external data shall be subject to centralized approval of the Bank, and this shall be included in outsourcing management system.	These are new requirements.
12	A Bank's collection of industry important data and core data from other banking and insurance institutions shall be approved by the NFRA.	
13	Data shall be mainly collected through the Bank's IT system. Other collection channels or temporary collection shall be limited or reduced.	
14	When using the Internet and other information networks to carry out data processing activities, a Bank shall implement the requirements of classified cyber security protection, security protection for critical information infrastructure, and password protection.	This should not raise additional obligations upon Banks, as it reinstates the existing requirements provided in other rules, such as the requirements of classified cyber security protection under the *Cybersecurity Law* (《*网络安全法*》) and the *Implementing Guidelines for Classified Protection of Cybersecurity in the Financial Industry* (《*金融行业网络安全等级保护实施指引*》).
15	Intragroup data sharing: ■ A firewall shall be established to segregate data between a Bank and its parent or group. ■ If a Bank shares sensitive data, important data or core data (not exclusive to personal information) with its parent or group, it shall obtain consent from data owners. ■ A Bank shall not terminate or refuse providing financial services on the ground that the data owner does not consent to sharing of sensitive data, unless the data shared is necessary for the provision of products or services.	These are new requirements and may cause the following complications: ■ If a Bank uses offshore servers run by its parent or affiliates, technically it may be difficult to achieve the segregation from its parent or group. ■ A Bank will need to obtain consent from corporate clients before sharing their sensitive data, important data and core data with its parent or group.

No.	Key requirements	Implications and actions
	General	
16	For entrusted processing, a Bank shall enter into contracts with service providers to agree on: ■ purpose, tenor, processing methods, data scope, security measures and each party's responsibilities and duties for data security, return or deletion of data, recordkeeping and audit; ■ no sub-delegation, sharing or use of data with third parties, without consent from the Bank.	The Bank will need to revisit existing service agreements and extend the relevant data security clauses to all data.
17	A Bank shall incorporate the data entrusted processing into the scope of IT outsourcing management and shall not outsource its responsibility for IT management and responsibility for data security to vendors, nor shall it outsource any functions involving IT strategic management, IT risk management, IT internal audit and other functions relating to IT core competitiveness to vendors. Compared to the Draft Measures, the Data Security Measures add a new requirement that where the supply chain services involve the processing of sensitive data, important data and core data, the Bank shall strengthen its management on the onboard and security of vendors.	These requirements are generally consistent with the provisions under the *Measures for the Regulation of Information Technology Outsourcing Risks of Banking and Insurance Institutions*(《银行保险机构信息科技外包风险监管办法》and the *Circular on Strengthening the Network and Data Security Management in Cooperation with Third Parties* (《关于加强第三方合作中网络和数据安全管理的通知》). Specifically, Banks should pay attention to the data security management of vendors, which has become a regulatory focus of NFRA.
18	The external provision of sensitive data, important data and core data shall be subject to data owners' consent, unless otherwise provided in laws and administrative regulations. The cross-entity flow of core data will be subject to risk assessment and security assessment.	The consent requirement is now applied to external provision of PI (as already required under the PIPL) and also all sensitive data, important data and core data. The risk assessment and security for cross-entity data flow is a new requirement but it is not expected to affect Banks given they do not process core data.
19	A Bank shall back up data properly and strengthen the protection of the sensitive data, important data and core data, and implement the separate storage of backup data and production data, and strictly manage the access control to backup data. A Bank is also required to formulate a backup plan, and ensure the completeness and effectiveness of backup data and recoverability of business.	Most requirements are already provided under existing national standards (e.g., the Financial Data Life Cycle Security Specification).

No.	Key requirements	Implications and actions
General		
Data security technology		
20	Access control: ■ user access shall match the relevant business need and data grading. ■ a Bank shall keep log of operations of sensitive data, important data and core data. ■ operational log of core data and its backup data shall be retained for at least 3 years. ■ operational log of important data and sensitive data and their backup data shall be retained for at least 1 year. ■ operational log of entrusted processing, joint processing and their backup data shall be retained for at least 3 years. ■ a Bank shall conduct audit on data operations every 6 months.	These are new requirements. Some of them are already provided under existing national standards (e.g., the Financial Data Life Cycle Security Specification).
21	A Bank shall have disaster backup for sensitive data, important data and core data, and verify data recoverability regularly.	
22	Other data lifecycle security measures	The Banking Data Governance Guidelines, the *Banking IT Risk Management Guidelines* (《*商业银行信息科技风险管理指引*》) and existing national standards (e.g., the Financial Data Life Cycle Security Specification and *Technical Specifications for Personal Financial Information Protection* (《*个人金融信息保护技术规范*》) have similar provisions.
PI protection		
23	A Bank shall conduct PI protection impact assessment for any business activity that involves processing of PI that may have material impact on the rights and interests of individuals, and the assessment record shall be retained for at least 3 years.	This echoes Art.55 of the PIPL.
24	In case of actual or potential PI risk event (leakage, tamper or lost), a Bank shall take remedial measures immediately, notify the relevant data owners and report to NFRA or its local offices. If the measures taken by a	This echoes Art.57 of the PIPL.

No.	Key requirements	Implications and actions
	General	
	Bank can effectively avoid any harm caused by the abovementioned PI risk events, the Bank may not notify the relevant data owners, provided however that where NFRA deems that any harm may be caused, they may require the Bank to notify the corresponding data owners.	
25	Other PI protection requirements	These are consistent with the PIPL.
	Data security risk monitoring and handling	
26	A Bank shall effectively monitor data threats, such as: ■ unauthorized access; ■ abnormal flow of sensitive data, important data and core data in different zones; ■ abnormal data processing or data leakage, lost or tamper by service providers; and ■ customer complaints on data security.	This is to implement the generic risk monitoring requirement under Art.29 of the DSL. Existing national standards (e.g., the Financial Data Life Cycle Security Specification) have similar provisions.
27	Risk assessment and audit: ■ bank shall conduct data security risk assessment every year. ■ audit department shall conduct full-scale data security audit every 3 years, and conduct special audit in case of a serious data security event.	This is to implement the generic risk assessment requirement under Art.29 of the DSL.
28	A Bank shall classify data security events into 4 levels – extremely serious, serious, relatively serious and general. The annex to the Data Security Measures provides the criteria for the classification of these 4 different levels of data security events.	This is a new requirement.
29	A Bank shall set up a reporting system for data security events, depending on the levels of data security events. A Bank shall also notify its clients and business partners in accordance with the terms of their agreements.	This is to implement the generic risk assessment requirement under Art.29 of the DSL. Existing national standards (e.g. the Financial Data Life Cycle Security Specification) have similar provisions.
30	Regulatory reporting: ■ upon occurrence of a data security event, a Bank shall report to NFRA or its local office within 2 hours and submit the formal written report within 24 hours. ■ in case of an extremely serious data security event, a Bank shall immediately take disposal measures, promptly notify users, and report to the local public	These are new requirements.

No.	Key requirements	Implications and actions
	General	
	security organ and NFRA or its local office. The Bank shall report to these authorities every 2 hours until the event is resolved. ■ when a data security event ends, Bank shall report to NFRA or its local office of such event, its assessment and improvement.	
	Supervision	
31	NFRA will conduct onsite and offsite inspections over the Bank's data security and incorporate data security in the regulatory rating system.	This is consistent with Art.50 and Art.52 of the Banking Data Governance Guidelines.
32	NFRA will formulate the catalog of important data, and propose suggestions for the catalogue of core data for the banking sector. Banks need to classify the data according to the abovementioned catalogs and submit the catalog of important data to NFRA or its local office, and file immediately with them any material changes to the catalog of important data.	Banks will need to classify the data according to such catalog and submit the catalog of important data (as amended) to NFRA. We understand NFRA will issue the catalog of important data in the banking sector soon.
33	NFRA will set up co-management mechanism with Cyberspace Administration of China ("**CAC**") and implement the sharing of data security information, risk monitoring and alerts, and disposal of data security events.	Banks shall also comply with the CAC data regulations.
34	With respect to data sharing, entrusted processing, transfer transactions and data transfer involving bulk of sensitive data, important data or core data, Banks shall report to NFRA or its local office 20 business days prior to such processing or signing of the relevant service agreement, unless otherwise provided by laws and administrative regulations.	Banks will need to report new service agreements involving sensitive data and important data to NFRA before data processing and agreement signing. It remains to be seen how "bulk" would be defined and whether this rule would have retrospective effect on existing service agreements.
35	A Bank shall submit annual data security risk assessment report to NFRA or its local office by 15 January in the next year.	This is a new requirement.
36	Violations of the provisions under the Data Security Measures would subject a Bank to the following regulatory measures: ■ risk warning, regulatory talk, regulatory announcement, order to make corrections; ■ order to suspend or terminate certain systems or	These are generally consistent with the *Banking Supervision Law* (*《银行业监督管理法》*).

No.	Key requirements	Implications and actions
	General	
	applications that involve violations; ■ monetary fines on the Bank in the range of RMB200,000 to RMB500,000, depending on the severity of the violation; ■ order to suspend business or revocation of business permits in cases of particularly serious circumstances or failure to rectify within the stipulated period; and/or ■ disciplinary actions may be imposed on directly responsible directors, senior management personnel, and other directly responsible persons depending on the severity of the violation; in case the wrongdoing does not constitute a crime, warnings and monetary fines may be imposed on the directly responsible directors, senior management personnel or other directly responsible persons in the range of RMB 50,000 to RMB500,000; the qualifications of directly responsible directors and senior management personnel may be cancelled for a certain period or for life term, and directly responsible directors, senior management personnel, and other directly responsible persons may be banned from the banking sector for a certain period or life term. If the wrongdoing constitutes a crime, criminal liabilities shall be pursued according to laws.	
	Miscellaneous	
37	Foreign bank branches were included in the Draft Measures but deleted from the Data Security Measures. However, the Data Security Measures generally provides that these measures shall apply, *mutatis mutandis*, to other banking financial institutions approved by NFRA.	Foreign bank branches (as within the scope of "other banking financial institutions") should also comply with the Data Security Measures where applicable to non-legal person entities.

2. CTA Update: BOI Reporting Obligation is Once Again Suspended

Author: Mike Chiang of Han Kun LLP

Summary

In a series of significant developments, the United States Court of Appeals for the Fifth Circuit has vacated its earlier stay on the preliminary injunction that had briefly reinstated the Corporate Transparency Act (CTA) Beneficial Ownership Information (BOI) reporting requirements. This decision marks another shift in the enforcement landscape, creating continued uncertainty for businesses across the country.

Timeline of events

- **December 3, 2024**

The U.S. District Court for the Eastern District of Texas issued a preliminary injunction, temporarily halting CTA enforcement due to constitutional concerns.

- **December 23, 2024**

The Fifth Circuit initially granted the government's motion for an emergency stay, effectively reinstating CTA requirements, citing the CTA's constitutionality under the Commerce Clause and the minimal compliance burden on businesses.

- **December 26, 2024**

The Fifth Circuit vacated its stay, reinstating the injunction against CTA enforcement to maintain the "constitutional status quo" while the appeal continues.

Impact on BOI reporting requirements and deadlines

BOI reporting obligation is once again suspended. Business entities are NOT required to file BOI reports in accordance with the following deadlines previously announced by FinCEN:

- **Pre-2024 Entities:** BOI filing deadline extended to January 13, 2025 (was January 1, 2025).
- **Entities with Filing Deadlines Between Dec 3–23, 2024:** Filing now due January 13, 2025.
- **Entities Formed Dec 3–23, 2024:** Additional 21 days granted for BOI filing.
- **Post-January 1, 2025 Entities:** No changes; must file within 30 days of creation or registration.

Further guidance from FinCEN or the courts will determine future obligations.

Key takeaways

- **Compliance Preparation:** Businesses may pause BOI filings but should remain prepared for potential changes.

- **Ongoing Legal Proceedings:** The expedited appeal process suggests resolution may come in early 2025.
- **Stay Updated:** Monitor developments as legal proceedings continue.

3. Strengthening Oversight of Imported Drugs: Key Takeaways into New Regulations on Domestic Responsible Entities

Authors: Aaron GU | Pengfei YOU | Duzhiyun ZHENG | Matt ZHANG | Franky YU | Shuwen SUN | Ariel YANG[2]

On November 13, 2024, the National Medical Products Administration (the "**NMPA**") issued the *Interim Provisions on the Management of Domestic Responsible Entity Designated by Overseas Marketing Authorization Holders* (hereinafter referred to as the "**Regulations on Domestic Responsible Entities**"). This regulation will officially take effect on July 1, 2025 and has garnered significant attention from the industry. The introduction of the Regulations on Domestic Responsible Entities represents a major milestone in the evolution of China's Marketing Authorization Holder (MAH) regulations. The new regulation aims to clarify and reinforce the responsibilities of MAH and domestic responsible entities for imported drugs, thereby enhancing the safety of public medication use. In this article, we analyze several key points of the Regulations on Domestic Responsible Entities from a practical perspective, with the aim of offering valuable insights and encouraging discussion within the industry.

Interpretation of key points

I. Domestic responsible entities vs. domestic agents

Previously, the entity designated by overseas MAH to fulfill MAH's obligations in China is referred to as the "domestic agent" in China's regulatory regulation[3]. This time, the Regulation on Domestic Responsible Entities has updated the concept of "domestic agent" to "domestic responsible entities". Similarly, the *Draft Measures for the Administration of Pharmaceutical Representatives* issued in November 2024 specifies that the "domestic responsible entity" designated by the MAH for imported drugs is responsible for fulfilling MAH obligations. The change in terminology not only underscores the responsibilities of domestic entities but also reflects innovative developments in regulatory concepts and requirements.

It is worth noting that domestic responsible entities must still adhere to the regulatory requirements previously applicable to domestic agents. These responsibilities include implementing drug recalls in accordance with *the Drug Recall Management Measures* and overseeing the filing and management of pharmaceutical representatives under *the Provisional Measures for the Filing of Pharmaceutical Representatives*.

II. Designation for domestic responsible entities

The roles of domestic responsible entities and registration agents are distinct. According to the Regulations on Domestic Responsible Entities, overseas MAHs are required to designate a domestic

[2] Jingjing XU have contributions to this article.

[3] The Article 20 of *the Drug Recall Management Measures*, the Article 4 of *the Provisional Measures for the Filing of Pharmaceutical Representatives*, the Article 2 of *the Draft Interim Provisions on the Management of Domestic Agents for Overseas Marketing Authorization Holders*, and the Article 44 of *the Draft for Comments on the Implementing Regulations of the Drug Administration Law of the People's Republic of China*.

responsible entity before the initial importation and sale of the drug[4]. However, there is currently no explicit requirement to designate a domestic responsible entity during the clinical trial or registration application stages. In contrast, a registration agent is a domestic legal entity authorized by the MAH during the drug registration application phase to handle matters related to drug registration[5]. Thus, domestic responsible entities and registration agents serve separate functions, each with its own set of responsibilities.

In practice, domestic responsible entities and registration agents can be different entities. For instance, based on our project experiences, if an overseas company has confidentiality concerns about submitting registration materials through a domestic partner, the domestic responsible entity role can be assigned to a distributor or other partner, while registration agent responsibilities can be entrusted to a CRO or other specialized service provider, with assistance from lawyers. This flexible arrangement not only helps safeguard confidentiality but also enables companies to navigate complex market dynamics and increasingly stringent regulatory requirements more effectively.

III. Drug insert sheet: domestic responsible entities and domestic contact entities

In accordance with the requirements of the Regulations on Domestic Responsible Entities, the name, address, and contact information of the domestic responsible entities must be clearly listed in the drug insert sheet[6]. Additionally, under the current *General Format and Writing Guidelines for Drug Insert Sheet of Chemical Drugs and Biological Products*, imported drugs must also include in their drug insert sheet the relevant information of the domestic contact entities in China designated by the overseas MAHs. Such information should include the name, registered address, postal code, telephone number, fax number, and other details.

The Regulations on Domestic Responsible Entities are set to take effect, and the current *General Format and Writing Guidelines for Drug Insert Sheet of Chemical Drugs and Biological Products* remains in force. Therefore, the relationship between the domestic responsible entity and the domestic contact entity has yet to be clarified. It remains uncertain whether the information of both entities will need to be listed in the drug insert sheet, along with their respective responsibilities, which are likely to be further clarified in subsequent regulations. Moreover, these uncertainties will also present new challenges for the drafting of drug insert sheets and impose higher requirements on corporate compliance and information disclosure.

IV. Selection and requirements for domestic responsible entities

The Regulations on Domestic Responsible Entities specifies the requirements for domestic

[4] The Article 5 of the *Regulations on Domestic Responsible Entities*: "Before the initial importation and sale of a drug, overseas holders shall report their designated domestic responsible entity to the drug regulatory authority of the province, autonomous region, or municipality where the domestic responsible entity is located via the National Drug Business Application System and upload the authorization materials for the designated domestic responsible entity".

[5] The Article 9 of the *Drug Registration Administration Measures (2020)*: "Applicants shall be enterprises or drug research institutions capable of assuming corresponding legal responsibilities. Overseas applicants shall designate a domestic legal entity in China to handle matters related to drug registration".

[6] The Article 7 of the *Regulations on Domestic Responsible Entities*: "…The name, address, and contact information of the domestic responsible entity should be listed in the drug insert sheet".

responsible entities, mandating that overseas MAHs carefully consider relevant entities' quality management systems, personnels, facilities, and capabilities to fulfill relevant joint obligations when designating domestic responsible entities. The Regulations on Domestic Responsible Entities also emphasizes the requirements of the domestic responsible entities should closely align with those of overseas MAHs. However, the specific criteria and qualifications for these requirements still need further clarification. For instance, it remains unclear whether employees with labor relations in other entities within the same group as the domestic responsible entities can meet the requirement of "having dedicated personnel solely responsible for drug quality management". Considering the Article 17 of the Regulations on Domestic Responsible Entities authorizes local drug regulatory authorities to issue further implementation rules, it is recommended that overseas MAHs closely monitor the issuance of the rules by the provincial drug regulatory authorities where the domestic responsible entities are located, in order to make timely adjustments and responses.

We particularly advise that overseas MAHs carefully evaluate their selection of domestic responsible entities to comply with the Regulations on Domestic Responsible Entities and relevant laws and regulations. Similarly, domestic responsible entities should thoroughly assess their existing conditions and capabilities, ensuring that both parties can effectively cooperate in fulfilling joint obligations and avoid potential legal risks.

V. Authorization and responsibility allocation for overseas MAHs

We recommend that overseas MAHs select entities that meet the requirements of the Regulations on Domestic Responsible Entities before its official implementation and prepare and notarize the authorization responsibility list in advance. Based on our observation, many multinational pharmaceutical companies have already begun drafting authorization responsibility list. It is also advisable to closely monitor the issuance of detailed regulations or official document templates. Meanwhile, overseas MAHs should promptly complete the authorization and system reporting for the domestic responsible entities and timely revise the drug insert sheets to avoid penalties resulting from non-compliance once the transition period ends. If overseas MAHs have not completed the system reporting for the domestic responsible entities by April 30, 2025 (the deadline for the annual drug reporting[7]), they may still submit information for the previous year through the original channels. Furthermore, considering that overseas MAHs and domestic responsible entities bear joint liability, we recommend that overseas MAHs clearly define responsibilities and distribute obligations through internal agreements.

At the same time, we would like to emphasize that the differentiation and determination of responsibilities between the MAH and the domestic responsible entity is still an area that requires careful observation. Specifically, it remains to be seen whether authorization responsibility list and internal agreements can effectively serve as "firewall" to mitigate risks during regulatory enforcement. However, overall, the clearer the allocation of responsibilities, the better it will assist regulatory

[7] The *Regulations on the Annual Reporting Management for Drugs*: "...The deadline for submitting the 2021 annual reporting information is August 31, 2022; starting from next year, the deadline for submitting the previous year's report information will be April 30 of each year".

authorities in accurately distinguishing responsibilities during enforcement and reducing ambiguity.

Conclusion

The issuance of the Regulations on Domestic Responsible Entities marks a significant step in the normalization of China's pharmaceutical regulatory framework. However, the specific standards for the relevant requirements are still being explored and will be gradually implemented by medical industry and regulatory authorities. As the global pharmaceutical market continues to open, China's pharmaceutical industry is poised to encounter unprecedented development opportunities. This will not only promote the export and import of innovative drugs, but also facilitate the introduction of advanced international technologies and resources, injecting new energy into the domestic pharmaceutical market. In the future, we anticipate that a more regulated, open, and dynamic Chinese pharmaceutical market, supported by an increasingly refined regulatory framework, and as exemplified by the Regulations on Domestic Responsible Entities, will be able to provide higher quality medical products and services to both domestic and overseas patients.

4. CTA Update: BOI Reporting Requirements Reinstated

Author: Mike Chiang of Han Kun LLP

On December 23, 2024, the US Court of Appeals for the Fifth Circuit issued an order in **Texas Top Cop Shop Inc. v. Garland**, granting the government's emergency motion for a stay pending appeal of the preliminary injunction that had paused enforcement of the Corporate Transparency Act (**CTA**). This order effectively reinstates the CTA's requirements, including the Beneficial Ownership Information (**BOI**) reporting requirements for many US entities.

Key highlights

- **Background:** December 3, 2024, the US District Court for the Eastern District of Texas issued a nationwide preliminary injunction, citing constitutional concerns, temporarily halting the enforcement of the CTA and its implementing regulations.
- **Fifth Circuit's rationale:** The appellate court found that the government made a compelling case for the constitutionality of the CTA under the Commerce Clause. It underscored the national interest in combating financial crimes and noted the minimal burden on businesses to comply with reporting requirements.
- **Stay granted:** With the preliminary injunction lifted, the BOI reporting obligations under the CTA are back in force, pending the resolution of the government's appeal.

New reporting deadlines announced by FinCEN

Recognizing the delay caused by the preliminary injunction, the Department of the Treasury's Financial Crimes Enforcement Network (**FinCEN**) has adjusted filing deadlines as follows:

- **Reporting companies formed or registered before January 1, 2024**: New deadline to file BOI reports is **January 13, 2025** (previously January 1, 2025).
- **Reporting companies created or registered on or after September 4, for which the initial filing deadline had been between December 3 and 23, 2024:** the new deadline to file the BOI report is **January 13, 2025**.
- **Reporting companies created or registered from December 3 to 23, 2024**: An additional 21 days from their initial deadline is granted.
- **No changes for reporting companies formed or registered on or after January 1, 2025**: These entities must file their BOI reports within 30 days of creation or registration.

Next Steps

- **Compliance:** Impacted reporting companies should resume gathering beneficial ownership data and ensure readiness for the revised deadlines.

- **Ongoing appeal:** The government's appeal will proceed expeditiously, with oral arguments expected early in 2025.
- **Monitoring updates:** Companies should stay informed as further legal developments may affect compliance obligations.

This holiday season, while many businesses enjoy a brief respite, the CTA compliance clock resumes ticking. We encourage all impacted entities to use this extension and prepare to meet their obligations under the CTA.

5. Han Kun Legal Updates on the Corporate Transparency Act (CTA)

Author: Mike Chiang of Han Kun LLP

Nationwide preliminary injunction suspends CTA enforcement

On December 3, 2024, the United States District Court for the Eastern District of Texas issued a nationwide preliminary injunction in *Texas Top Cop Shop, Inc. et al. v. Garland*, temporarily halting the enforcement of the Corporate Transparency Act (**CTA**) and its implementing regulations. This development has significant implications for reporting companies required to file Beneficial Ownership Information (**BOI**) reports under the CTA. Below is an analysis of the key aspects of this ruling and its implications.

Overview of reporting obligations under the CTA

The CTA, effective January 1, 2024, introduces new disclosure requirements for many U.S. entities. A **reporting company** is broadly defined as any domestic or foreign entity created by filing a document with a secretary of state or similar office, or registered to do business in the United States, unless exempt. Key reporting obligations include:

I. Who must report

Reporting companies, unless exempt, include corporations, LLCs, and similar entities. Exempt entities include publicly traded companies, certain regulated entities (e.g., banks, credit unions, insurance companies), and entities meeting specific operational criteria (e.g., at least 20 full-time employees and $5 million in gross receipts).

II. What to report

Reporting companies must provide:

- **Beneficial owners**: Individuals owning or controlling at least 25% of the reporting company or exercising substantial control.
- **Company applicants**: Individuals responsible for filing the reporting company's formation or registration documents.

III. When to report

- Reporting companies formed **before January 1, 2024**, must file their initial BOI report by **January 1, 2025**.
- Reporting companies formed **on or after January 1, 2024**, must file their BOI report within **90 calendar days of formation or registration**.
- Reporting companies formed **on or after January 1, 2025**, must comply with the **30-day filing requirement**.

Penalties for non-filing

Failure to comply with the CTA's BOI reporting requirements can lead to significant penalties:

1. **Civil penalties**: As of 2024, a reporting company that fails to file, submits false information, or fails to update its BOI as required may face civil penalties of up to **$591 per day** for each day the violation continues.
2. **Criminal penalties**: Willful failure to report accurate BOI or knowingly submitting false or fraudulent information can result in **criminal fines of up to $10,000** and/or imprisonment for up to **two years**.

Court's grounds for the ruling

The court granted the preliminary injunction based on the following:

1. **Federal overreach**: The CTA interferes with state authority over corporate governance, violating the Tenth Amendment.
2. **Compelled disclosure**: Requiring sensitive ownership data disclosure infringes on First Amendment rights.
3. **Privacy violations**: The CTA mandates disclosures without adequate safeguards, violating Fourth Amendment protections.
4. **Overbroad scope**: The Act imposes disproportionate burdens on small businesses unrelated to financial crimes.
5. **Likelihood of unconstitutionality**: The court found a strong basis to conclude the CTA likely violates constitutional protections.

Impact of the injunction

1. **Compliance obligations on hold**: Reporting companies are temporarily relieved from filing BOI reports until further legal proceedings determine the outcome of the injunction.
2. **Suspension of penalties**: Civil and criminal penalties for non-compliance are paused during the injunction period.
3. **Future developments**: If the injunction is overturned, reporting companies may need to act quickly to meet compliance obligations. Maintaining accurate ownership records is strongly advised.

Looking ahead

The preliminary injunction provides temporary relief but does not diminish the significance of the CTA's objectives. Reporting companies should remain vigilant and prepared for potential changes in enforcement. Han Kun Law Offices will monitor developments and provide timely updates as the situation evolves.

Important Announcement

This Newsletter has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Beijing	**David LI**	**Attorney-at-law**
	Tel:	+86 10 8525 4668
	Email:	david.li@hankunlaw.com
Shanghai	**Kelvin GAO**	**Attorney-at-law**
	Tel:	+86 21 6080 0920
	Email:	kelvin.gao@hankunlaw.com
Shenzhen	**Jason WANG**	**Attorney-at-law**
	Tel:	+86 755 3680 6518
	Email:	jason.wang@hankunlaw.com
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com
Haikou	**Jun ZHU**	**Attorney-at-law**
	Tel:	+86 898 3665 5000
	Email:	jun.zhu@hankunlaw.com
Wuhan	**Jiao MA**	**Attorney-at-law**
	Tel:	+86 27 5937 6200
	Email:	jiao.ma@hankunlaw.com
Singapore	**Lan YU**	**Attorney-at-law**
	Tel:	+65 6013 2966
	Email:	lan.yu@hankunlaw.com
New York	**Mike CHIANG**	**Attorney-at-law**
	Tel:	+1 646 849 2888
	Email:	mike.chiang@hankunlaw.com