HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

Han Kun Newsletter

Issue 226 (2nd edition of 2026)

Legal Updates

1. Key Takeaways from Notice No.42: New Regulatory Measures on Virtual Currencies in the Chinese Mainland

Authors: Kanxi LIAO | Yan XIA | Ye LI | Weiyu CEN

On 6 February 2026, eight PRC authorities, including the People's Bank of China, jointly issued the Notice on Further Preventing and Addressing Risks Related to Virtual Currencies and Other Matters ("**Notice No.42**"). On the same day, the China Securities Regulatory Commission ("**CSRC**") issued the Regulatory Guidelines on the Offshore Issuance of Asset-Backed Securities Tokens Backed by Onshore Assets (the "**RWA Issuance Regulatory Guidelines**"). Notably, Notice No.42 repeals the 2021 Notice on Further Preventing and Disposing of Risks of Speculation in Virtual Currency Trading (Yinfa [2021] No.237, the "**No.237 Notice**"), which had previously served as the principal framework document governing virtual-currency-related activities in the Chinese Mainland. Although Notice No.42 largely preserves the existing regulatory approach, it also introduces several significant adjustments. This article highlights the key changes brought about by Notice No.42.

Policy Background and Regulatory Tone

Financial regulation in the PRC is characteristically practice-driven: regulatory measures are often calibrated through normative documents and policy guidance in response to new market developments and emerging risks. Since 2025, speculative activities relating to virtual currencies have again intensified in the Chinese Mainland, with certain market participants using real-world asset ("**RWA**") tokenization as a promotional theme and a vehicle for speculation.

Against the broader objective of maintaining social stability and financial order, Notice No.42 was issued together with the RWA Issuance Regulatory Guidelines. Together, these measures both reaffirm the existing risk-control framework and provide more targeted regulatory responses to emerging structures such as RWA.

Continuation of the Existing Regulatory Framework

Overall, Notice No.42 continues the existing regulatory framework, and much of its wording tracks the No.237 Notice. The key points include:

1. Legal characterization: virtual currencies do not have the legal status of currency.
2. Nature of the business: virtual-currency-related business activities conducted within the Chinese Mainland constitute illegal financial activities and remain subject to a blanket prohibition.
3. Third-party involvement: onshore financial institutions, internet companies and other third parties must not provide services for virtual-currency-related activities.
4. Mining-related activities: existing mining projects remain subject to inspection and shutdown, while new mining projects are strictly prohibited.

5. Civil-law consequences: the relevant civil juristic acts are void, and any resulting losses must be borne by the parties themselves.

6. Liability of onshore persons: where an onshore person knows or should know that an offshore entity is illegally providing services into the Chinese Mainland but nevertheless provides assistance, such person may be held liable.

Key Changes, Primarily from a Cross-Border Perspective

Most notably, Notice No.42 introduces three important changes.

I. New Requirement (Article 13): Absent Regulatory Approval, Onshore Entities and Their Controlled Offshore Entities Must Not Issue Virtual Currencies Offshore

This is a substantive and highly consequential new requirement. Previously, while the No.237 Notice expressly prohibited "token issuance financing", it did not clearly distinguish between onshore and offshore issuance. In practice, enforcement focused primarily on activities carried out within the Chinese Mainland. Some onshore parties sought to circumvent the existing framework by establishing or controlling offshore vehicles and using those vehicles to conduct token issuance and fundraising offshore. Notice No.42 now makes clear that the regulatory reach extends offshore and adopts an approach that focuses on the identity and control nexus of the relevant entity, rather than solely on the place where the conduct occurs. In other words, an offshore issuance may still fall within the regulatory scope of the Chinese Mainland where the issuer is linked to an onshore party through control.

This provision has two principal dimensions:

- **Regulated subjects: "onshore entities and their controlled offshore entities"**

Although Notice No.42 does not define "onshore entities", a holistic reading of the text suggests that both onshore entities and onshore individuals are intended to be covered. The concept of "control" is central to this framework and serves as the basis for look-through supervision. In our view, "control" should not be limited to equity ownership, but may also extend to de facto control, material influence, or benefit direction exercised through contractual arrangements, nominee holding structures, technological dominance, operational decision-making, or other means that confer substantive influence over key matters. This approach effectively combines person-based jurisdiction with look-through jurisdiction and is designed to prevent circumvention through complex offshore structures–for example, by establishing or controlling, or arranging for third parties to hold interests in, companies incorporated in jurisdictions such as the British Virgin Islands, the Cayman Islands or Singapore, and using such structures to issue virtual currencies offshore.

Because "control" is not expressly defined in Notice No.42, determining whether control exists may require a more nuanced, fact-specific analysis in practice, particularly for offshore structures commonly used in token projects, such as foundations and DAOs (decentralized autonomous organizations). In the case of foundations, relevant factors may include governance arrangements, board composition and voting mechanisms, sources of funding, economic arrangements (including benefit distribution),

and the identity of the party initiating or leading the project. In the case of DAOs, the analysis may require tracing the initial allocation of governance tokens, identifying the initiators of key proposals, assessing the concentration of voting power over major decisions, and considering other comparable indicators. Where an onshore party is the principal initiator of a project and controls the early governance rights or a substantial portion of the tokens, regulators may take the view that the onshore party is effecting an offshore issuance through its control of the DAO. Alternatively, because a DAO may lack conventional legal personality, regulators may take a look-through approach and treat the onshore party as directly conducting the offshore issuance.

Separately, where an onshore party invests in an offshore issuer without controlling it, other forms of liability may still arise depending on the facts. For example, if the relevant token project is promoted to, or raises funds from, persons in the Chinese Mainland, then an onshore party that provides assistance–such as endorsement, traffic diversion or technical support–may still be found liable under Article 18 of Notice No.42 on the basis that it knew or should have known that the project was unlawful.

- **Regulated conduct: "issuing virtual currencies offshore"**

Notice No.42 expressly identifies the place of issuance as "offshore", thereby bringing issuance activities conducted anywhere in the world–including in Hong Kong–within the potential scope of regulation. A key practical question, however, is how "issuance" will be interpreted.

In addition to direct issuance structures such as ICOs (initial coin offerings), IEOs (initial exchange offerings) and IDOs (initial DEX offerings), many Web3 teams raise funds through instruments such as SAFTs (simple agreements for future tokens), SAFEs (simple agreements for future equity) combined with token warrants, and similar arrangements. Under these structures, tokens are not issued immediately; rather, the arrangements typically involve a pre-sale, a commitment to deliver tokens in the future, or the grant of a future subscription right. Applying a substance-over-form approach, regulators may not treat "issuance" as a purely formal, point-in-time event. Instead, they may look through the entire issuance chain and focus on the substance of the conduct, viewing "issuance" as encompassing not only the ultimate creation and sale of the virtual currency itself, but also pre-sale and fundraising activities undertaken for the purpose of a future token issuance. On that basis, such fundraising structures may also fall within the regulatory perimeter.

In addition, Notice No.42 upgrades the prohibited conduct from "token issuance financing" under the No.237 Notice to the broader concept of "issuing virtual currencies". That drafting change could materially broaden the scope of affected projects. This is because issuance is not limited to financing-driven issuances; it may also include non-financing issuances (such as free airdrops and ecosystem incentive distributions) and functional issuances (such as employee incentive tokens, governance tokens and platform utility/fuel tokens). In our view, Notice No.42 may therefore bring both non-financing and functional issuances within the regulatory perimeter, rather than confining regulation to financing-type issuances only. The likely rationale is that, regardless of the issuer's initial purpose, tokens may subsequently flow into secondary trading or payment and settlement scenarios that are themselves prohibited. For example, "free" employee incentive tokens may, once sold by employees, generate economic effects similar to those of a financing issuance. From a risk-control perspective,

prohibiting issuance at the source is the most effective way to eliminate arguments that non-financing issuance is somehow permissible.

- **Exception: "unless approved by the relevant authorities in accordance with laws and regulations"**

Although this wording formally leaves room for legality, in practice it suggests that ordinary commercial projects are highly unlikely to obtain such approval. Its legislative logic appears closer to "prohibition as the rule, exceptional approval only", effectively foreclosing the relevant activities in substance.

II. Revised Formulation for Cross-Border Services: from "Prohibiting Services to Mainland Residents" to "Prohibiting the Illegal Provision of Services to Onshore Entities"

Despite the change in wording, we understand that the core regulatory expectation remains the same: offshore entities must not target persons in the Chinese Mainland by marketing to them, soliciting them, or providing them with relevant services. In practice, the question of who constitutes an "onshore entity" has long been a key compliance issue for offshore licensed virtual-asset institutions, including those in Hong Kong, particularly in the context of onboarding and KYC documentation requirements. Given the close connections between Hong Kong and the Mainland, striking an appropriate balance between compliance and business needs remains a practical challenge.

At the same time, the addition of the qualifier "illegal" raises the question whether some forms of cross-border services might still be lawful. Our preliminary view is that stablecoin-related services provided by offshore payment institutions within cross-border payment rails may potentially fall within a carve-out. There is meaningful commercial demand for such services in practice, and they do not appear to be the primary focus of the current enforcement framework. From an operational perspective, however, specific projects should still be assessed on a case-by-case basis.

III. Clarification of the RWA Regulatory Approach: "Prohibition of Onshore Activities" Plus "Approval for Offshore Issuance"

Notice No.42 adopts a broad, catch-all definition intended to capture different forms of RWA-related activities and strictly prohibits RWA activities conducted onshore. At the same time, where onshore assets are used for offshore RWA issuance, Notice No.42 adopts an approval-based framework.

For a more detailed discussion, please refer to our previous article, "Han Kun Insight | New Rules on Real-World Asset (RWA) Tokenization: A New Turn in the Road".

Beyond the foregoing, Notice No.42 also reflects several other adjustments. Article 1 effectively places a substantive brake on RMB stablecoin-related initiatives, thereby cooling the overheated market narrative seen in 2025. Article 15 requires offshore subsidiaries and branches of PRC-funded financial institutions to conduct RWA business in a "prudent" manner–a deliberately restrained formulation that also appears intended to temper market speculation–and to satisfy relevant conditions such as professional staffing and AML management. In addition, Articles 6 and 15 expressly mention intermediaries (including law firms and accounting firms) for the first time and make clear that they must not unlawfully provide services for illegal business activities. This appears to be a direct

response to the sharp increase in intermediary involvement over the past year.

Broader Implications: How to View Notice No.42 from a Global Perspective

From a global perspective, Notice No.42 reaffirms the Chinese Mainland's regulatory trajectory in relation to digital assets (virtual currencies). Unlike jurisdictions such as the United States, the European Union, Singapore and Hong Kong–which have been moving toward classification-based regulation and licensing regimes–the Chinese Mainland continues to adopt a risk-first approach under which prohibition remains the default position. The policy emphasis remains on preserving social stability and containing systemic financial risk.

Against this backdrop, the Chinese Mainland's stringent approach has, objectively, created a more distinct institutional space for Hong Kong. As a jurisdiction operating under the common law within the national framework, with a highly open capital regime and an already established licensing regime for virtual assets, Hong Kong has continued–on the premise that risks remain controllable–to advance the licensing of virtual asset trading platforms, the development of a stablecoin regulatory framework, and the exploration of RWA initiatives, thereby serving as something of a regulatory testing ground. In particular, in the context of intensifying strategic competition between China and the United States, it is not realistic for the country to remain entirely absent from the development of crypto assets and on-chain finance. Hong Kong's continued experimentation therefore helps preserve, while maintaining clear risk boundaries, an institutional interface and a degree of strategic flexibility for national participation in the global digital-asset industry, and places Hong Kong in a stronger position to capture structural opportunities in the compliant digital-asset sector.

2. MOFCOM Announces Tiered Listing of 40 Japanese Entities, Significantly Tightening Japan-Related Export Compliance

Authors: Ruixin JIANG | Yi XIONG

On 24 February 2026, the Ministry of Commerce of the People's Republic of China ("**MOFCOM**") issued Announcement No.11 and Announcement No.12 of 2026, simultaneously adding a total of 40 Japanese entities to the Export Control List and the Watch List, respectively. Earlier, on 6 January 2026, MOFCOM had already issued Announcement No.1 of 2026, which imposed broader export control rules on exports of dual-use items to Japan involving Japanese military end users, military end uses, and other end users/end uses that may contribute to enhancing Japan's military capabilities. With these three regulatory measures now in effect concurrently, compliance standards applicable to China-based companies' exports to Japan have become materially more stringent, and regulatory scrutiny has tightened further. In this context, relevant companies face more severe compliance challenges and should strengthen compliance management to ensure that Japan-related export business is conducted in strict accordance with applicable laws and regulations.

Overview of the Announcements and Updated Lists

Based on MOFCOM Announcements No.11 and No.12 (both issued on 24 February 2026), together with MOFCOM's spokesperson's same-day response to media questions regarding these Japan-related export control measures, the key rules and the latest adjustments to the Control List and Watch List are summarized below.

I. MOFCOM Announcement No.11 of 2026

- **Nature of list:** Export Control List. Once an entity is added to this list, exports of dual-use items to that entity are prohibited.
- **Reason for listing:** 20 entities were found to have directly participated in enhancing Japan's military capabilities.
- **Control measures:**
  - Chinese export operators are prohibited from exporting any dual-use items to such entities;
  - Overseas organizations and individuals are prohibited from transferring or providing China-origin dual-use items to such entities;
  - All ongoing related export and transfer activities must stop immediately;
  - Exports may be permitted only under special circumstances, subject to a separate application to MOFCOM.
- **Removal mechanism:** The announcement does not expressly provide a delisting mechanism for entities on the Control List. This, however, does not necessarily mean permanent listing. Going forward, MOFCOM may, based on actual circumstances and in light of the principles and spirit of

Article 18 of the Export Control Law and Article 30 of the Regulations on Export Control of Dual-Use Items, consider delisting applications by reference to factors such as changes in the international situation and corrective actions by the listed entities.

- **Listed entities:**

https://www.mofcom.gov.cn/zcfb/zc/art/2026/art_a73f2b59e13d4454b0f58618917f3944.html

II. MOFCOM Announcement No.12 of 2026

- **Nature of list:** Watch List. Entities placed on this list are not completely prohibited from receiving exports of dual-use items, but will be subject to more stringent and granular export review procedures.
- **Reason for listing:** 20 entities were listed because their end users and end uses for dual-use items could not be effectively verified.
- **Control measures:**
  - Exports to such entities are ineligible for a general license and cannot rely on the information–registration filing mechanism to obtain export certificates; only an individual license may be applied for;
  - Applications for an individual license must include an entity-specific risk assessment report and a written undertaking that the items will not be used to enhance Japan's military capabilities;
  - The license review period is not subject to the statutory time limit, and MOFCOM will conduct more stringent end-user and end-use review;
  - Exports involving Japanese military end users or military end uses, as well as any other end users or end uses that may contribute to enhancing Japan's military capabilities, will not be approved;
  - Pursuant to Article 28 of the Regulations on Export Control of Dual-Use Items, where a listed entity violates end-user/end-use management requirements or may endanger national security and interests, the competent commerce authority under the State Council may place it on the Control List and remove it from the Watch List.
- **Removal mechanism:** Pursuant to Article 26 of the Regulations on Export Control of Dual-Use Items, an entity may apply to be removed from the Watch List after fulfilling its obligation to cooperate with verification, provided verification confirms that it has not changed end use without authorization, transferred items to a third party without authorization, or otherwise engaged in relevant non-compliant conduct.
- **Listed entities:**

https://www.mofcom.gov.cn/zcfb/zc/art/2026/art_a73f2b59e13d4454b0f58618917f3944.html

Key Features and Implications of the Control/Watch Lists

I. Profile of Entities Covered by the MOFCOM Announcement No.11 List

The 20 entities placed on the Control List are all entities directly involved in enhancing Japan's military capabilities. Their business activities broadly span core sectors such as defense manufacturing, military electronics, military R&D, and military talent training. Several heavy-industry enterprises are exclusive or core manufacturers of major Japan Self-Defense Forces equipment and hold dominant positions in key fields such as naval vessels, military aircraft, aero engines, and military power systems. Several electronics/information enterprises serve as core technology and equipment suppliers for command-and-control communications, radar guidance, military satellites, and electronic warfare systems. The list also includes core institutions for military research and talent development in Japan. The controls imposed on these entities reflect a comprehensive blocking and isolation approach targeting the upstream segments of Japan's defense industry.

II. Profile of Entities Covered by the MOFCOM Announcement No.12 List

The 20 entities placed on the Watch List were listed because the end users and end uses of dual-use items could not be verified. Although these entities are not necessarily directly military in nature, they include leading enterprises and research institutions across various civilian sectors in Japan and present significant potential military-civil fusion conversion risk. Where supply-chain destination flows are uncertain, dual-use items may readily be diverted to military uses.

From an industry perspective, the relevant entities span automobiles, electronics, materials, aerospace supporting industries, chemicals, machinery, and trading. Their civilian products and technologies significantly overlap with military applications. For example, automotive engine and chassis technologies may be adapted for military vehicles; heavy machinery may be used in defense equipment manufacturing; and specialty oils and chemical reagents may support military production. In addition, certain listed research institutions conduct research in areas such as materials technology, semiconductor technology, and small adaptive drone technology–fields with potential military conversion value. In the absence of clear evidence regarding the downstream use of research outputs, such institutions may be included on the Watch List.

III. Impact on Exporting Enterprises

First, there is the impact on existing transactions. If a company's counterparty is included in the Control List under MOFCOM Announcement No.11, the transaction may be effectively interrupted. For example, executed contracts may need to be terminated unilaterally, potentially giving rise to subsequent disputes over breach damages. If a company continues trading on a speculative basis, regardless of intent, it may face severe administrative liability under the Export Control Law and related regulations, and criminal liability in serious circumstances.

By contrast, where a counterparty is included in the Watch List under MOFCOM Announcement No.12, export license application procedures will become more complex and stringent, materially affecting export timelines and operational efficiency. The additional review materials and the practical extension of review timelines may delay shipment schedules and ultimately affect timely contractual

performance.

Second, there is the impact on future routine exports to Japan. Implementation of these announcements means Japan-related exports are entering a phase of high-frequency scrutiny. Any company engaged in exports to Japan should conduct prudent assessment–even where the customer is a research institution or appears unrelated to defense on its face–to avoid regulatory obstacles arising from unclear end uses or other compliance concerns. In addition, under the Watch List mechanism, regulators may conduct more detailed review of relevant entities, impose more stringent documentation requirements, and substantially lengthen review timelines, all of which may have knock-on effects on pricing and delivery.

Third, there is a structural impact on corporate compliance management. These announcements accelerate a shift in export control compliance management from passive to proactive, and from ex post to ex ante control. This increases compliance costs, but also requires companies to structurally redesign their internal compliance governance. Compliance should no longer be treated merely as a remedial tool for post-incident accountability. Instead, it should be integrated into front-end management and corporate governance arrangements, embedded into the company's management system, and recognized not as a regulatory burden but as an integral component of sound corporate governance.

Compliance Recommendations for Enterprises

Based on the above summary and analysis, we set out below several compliance recommendations for enterprises directly or indirectly engaged in export business, for reference.

I. Conduct an Urgent and Comprehensive Review of Existing Business

1. Map and screen downstream customers (including direct and indirect customers)

Confirm, on a customer-by-customer basis, whether they are included in the current Control List or Watch List, and classify them for management purposes based on the screening results.

For customers on the Control List, urgently review the specific requirements and contractual arrangements under executed contracts, and discuss potential breach-dispute risks and response strategies with professional advisors in advance.

For customers on the Watch List, comprehensively review the status of existing license applications, supplement materials under the new rules (including entity-specific risk assessment reports and written end-use undertakings), and proceed only after license approval is obtained.

2. Review contracts currently under performance

Focus on whether there are unfavorable provisions or breach risks in relation to conditions precedent/conditions for performance tied to export license approval, compliance carve-outs/exemptions, and breach indemnity clauses. Where necessary, communicate appropriately with counterparties in advance to mitigate the risk of disputes.

II. Strengthen End-to-End Risk Control for Routine Export Business

1. Establish a customer due diligence mechanism

Implement a front-end customer review process, particularly for customers in sensitive jurisdictions. Review targets should include agents, distributors, and end users. Review scope should include qualifications, shareholding structure, business scope, military nexus, and associations with listed entities. Retain due diligence materials and reports, and assign risk ratings based on the results.

2. Optimize export license application management

For Watch List customers, establish a dedicated individual-license application workflow and a checklist of required application materials to ensure completeness, authenticity, and compliance. Where appropriate, prepare standardized templates for risk assessment reports and written undertakings to improve application efficiency.

3. Improve controls over license use

Maintain a license register (ledger) specifying each license's validity period, scope of application, and corresponding goods flow. Ensure that item descriptions, specifications, quantities, consignor/consignee information and other details on the license match the actual goods and customs declaration documentation.

4. Strengthen supply chain monitoring

Investigate whether goods may ultimately flow to listed entities through third-country transshipment, intermediary resale, or similar arrangements. Clearly allocate compliance obligations to upstream and downstream counterparties, and execute supplemental agreements where necessary. Retain documentary evidence of goods flow. If subsequent violations are identified (e.g., improper end use or unauthorized transfer), immediately suspend further cooperation and consult professional advisors in advance regarding response strategies.

5. Upgrade contract management

In light of the latest export control requirements, conduct compliance review of all procurement, sales, and entrusted-service contracts. Assess whether any provisions are unfavorable under current laws and policies, and add or revise compliance clauses where appropriate to reduce breach risks arising from changes or updates in export control laws and policies.

III. Improve the Export Control Compliance Management System

1. Formulate compliance policies and procedures

By reference to applicable laws, regulations, and policy requirements, formulate a tailored export control compliance management system, including role allocation, risk assessment workflows, customer review standards, document retention requirements, and violation-handling mechanisms.

2. Clarify compliance responsibilities and roles

Designate dedicated compliance personnel responsible for policy tracking, customer screening,

license applications, supply chain monitoring, and records management. At the same time, strengthen compliance coordination with sales, customs declaration, procurement, production, and other departments to ensure alignment and implementation of compliance requirements across all functions.

3. Conduct compliance training

Provide export control compliance training covering fundamental concepts and key requirements under recent rules, with a focus on dual-use item identification, listed-entity screening, license application procedures, and consequences of non-compliance. Conduct post-training assessments to ensure training effectiveness.

4. Conduct periodic compliance self-assessments

Establish a standing compliance risk identification and remediation mechanism, and carry out regular self-assessments of export business to identify and rectify potential risks in a timely manner. Where appropriate, engage external professional advisers to help strengthen compliance management, optimize compliance processes, and ensure the compliance system remains aligned with regulatory requirements.

3. From Fragmentation to Fortress: Regulatory Restructuring and Implications for PRC Banks' Cross-Border Transactions Under CRD 6

Authors: Han Kun Law Offices: Meng YAN | Yunjia SUN | Yueyun ZHANG
Han Kun LLP: Chengrong LI (Paul LI) | Chun Hei CHU (Samson CHU) | Yan Tung SO (Jane SO)

The EU's Capital Requirements Directive VI (Directive (EU) 2024/1619, "**CRD 6**" or the "**Directive**") entered into force on 9 July 2024 and will be fully implemented from 11 January 2027, introducing authorisation and compliance requirements for branches of third-country institutions.

Under the Directive, any non-EU bank that provides "core banking services" within the EU must establish a branch in the relevant EU Member State and apply to the local regulatory authorities for authorisation to provide such services, unless it provides such services through an EU-subsidiary. This means that third-country banks that previously relied on Member State legal exemptions to provide cross-border financial services will no longer enjoy such market-entry convenience. At the same time, EU branches of third-country banks will be brought into a unified minimum EU supervisory framework, covering key dimensions such as capital adequacy, liquidity buffers, and internal governance. Together, CRD 6 and Regulation (EU) 2024/1620 (CRR 3) form a package of EU banking regulation.

In response to the challenges CRD 6 presents for cross-border operations in the EU, this article outlines the relevant regulatory framework, key compliance risks for Chinese banks, and practical response strategies.

Core Changes in the CRD 6 Regulatory Framework

The introduction of CRD 6 marks a shift in EU financial regulation toward a geopolitically driven approach. In substance, the new rules are reshaping the EU's "financial border".

For many years, due to the lack of unified standards, EU Member States took divergent approaches to third-country bank access: some countries, aiming to attract foreign banks, offered broader regulatory exemptions and simplified procedures for obtaining a licence, while others applied stringent standards akin to those for EU subsidiaries. As a result, third-country banks used more lenient regulatory jurisdictions as a springboard to conduct low-cost operations. This type of "regulatory arbitrage" left EU subsidiaries that complied strictly with local rules at a competitive disadvantage. CRD 6 seeks to end this situation by harmonising the regulatory standards for EU operations of third-country banks and creating a level playing field.

A deeper shift is the reclaiming of regulatory sovereignty. In the past, EU regulators largely relied on home-country regulators of third-country banks (e.g., in China, the U.S., and the U.K.) and off-site monitoring. CRD 6 changes this logic by granting the European Central Bank and national regulators direct powers to intervene in the organisational structures of third-country branches. The EU's concern is that if the asset profile of a third-country bank's EU branch become too large (for example, breaching the €40 billion threshold), financial distress in the bank's home country could quickly be transmitted into Europe through cross-border channels. Therefore, the EU considers it necessary to have concrete

powers to manage risks in order to safeguard financial stability in Europe.

Key Interpretation of Article 21c of CRD 6

I. Scope of "core banking services"

Under Article 21c, the following cross-border services or products provided by non-EU credit institutions constitute banking services regulated by CRD 6:

1. taking deposits and other repayable funds;
2. lending, including but not limited to: consumer credit, credit related to immovable property, factoring with recourse, non-recourse factoring, and commercial transaction financing (including forfaiting);
3. guarantees and commitments.

For bank guarantees, standby letters of credit, and financing commitments, EU regulators generally view these products as essentially equivalent to credit support. Therefore, if a non-EU bank that does not have an authorised branch or subsidiary provides such products to a beneficiary or guaranteed party located in the EU, this will highly likely be considered a breach of the relevant provisions of Article 21c.

II. Determination of "carrying out business in a Member State"

Notably, CRD 6 does not provide an EU-level unified legal definition or criteria for determining whether a bank is "carrying out business in a Member State".

This ambiguity may create uncertainty in practice: for example, to what extent technical factors–such as the governing law of a facility agreement, the place of execution, or whether the setting up of a disbursement account is within the EU–might lead to a finding that core banking services are being provided in a Member State?

In the absence of EU-wide benchmarks, the decision making power is in effect devolved to Member State authorities. Differences in regulatory approach may lead to divergent outcomes across jurisdictions. Therefore, it is critical to examine how each Member State transposes CRD 6 into domestic law.

That said, returning to the legislative purpose of CRD 6 and its risk-control rationale, we tend to believe that whether a non-EU bank's cross-border business constitutes "carrying out business in a Member State" essentially depends on a holistic assessment of the following three core factors:

1. Whether the borrower is located in the EU, i.e., where the credit relationship is substantively anchored;
2. The continuity and systematic nature of the business, i.e., whether the bank is extending credit to EU entities on a non-incidental, ongoing basis; and
3. The functional nature of the activity, i.e., whether it falls within the bank's core functions for generating profit and assuming risk.

Accordingly, in general, where a customer or counterparty is located within the EU, the business may be treated as "being carried out in that Member State". In a typical cross-border credit scenario: if a Chinese bank outside the EU lends to a Chinese subsidiary established in the EU, even if approval processes, funds disbursement, and risk management are performed outside the EU, such transaction, unless exemption applies, will very likely be "looked through" and treated as "being carried out in a Member State" because the borrower and the financing purpose are anchored in the EU.

III. Exemptions

1. Legacy contracts

CRD 6 requires Member States to implement measures to protect rights already obtained by customers under contracts signed before 11 July 2026. In principle, such contracts do not trigger the requirement to establish a third-country branch due to the implementation of CRD6[1].

However, it should be noted that CRD 6 explicitly emphasises that legacy contracts are to be interpreted restrictively, so as to prevent evasion of regulatory oversight[2]. For material amendments, renewals, or extensions after 11 July 2026, there is significant uncertainty as to whether the exemptions still apply. It is expected that most Member States are likely to treat such changes as outside the exemptions.

2. Reverse solicitation

If an EU customer or counterparty requests for services entirely on its own exclusive initiative, the third-country institution may in principle be exempt from the branch requirement[3]. However, such exemption contains strict limitations: the third-country institution must not engage in any direct or indirect marketing, including through affiliates or third parties, to solicit customers. In addition, reverse solicitation covers only the specific product or service requested by the customer. The third-country institution cannot rely on the customer's request to promote other types of banking services unless they are follow-on services that are "necessary for, or closely related to" the originally requested service[4].

3. MiFID investment services and ancillary activities

Where a third-country institution provides core investment services under MiFID, CRD 6 does not apply to ancillary activities carried out in connection with those services, such as deposit-taking and lending related to the investment services[5].

Nevertheless, this exemption is conditional on the third-country institution being entitled to provide the relevant MiFID investment services legally in the EU. In practice, the scope for third-country institutions to provide MiFID services directly without obtaining EU authorisation is limited, making the

[1] See CRD 6, Article 21c.5.
[2] See CRD 6, Recital (6).
[3] See CRD 6, Article 21c.2(a).
[4] See CRD 6, Article 21c.3.
[5] See CRD 6, Article 21c.4.

practical applicability of the exemption rather narrow[6].

4. Interbank transactions

If the customer or counterparty is an EU credit institution, the third-country institution may be exempt when providing core banking services[7]. This leaves some room for traditional interbank transactions.

For secondary loan market transaction structures such as participations, these may be initially regarded as providing services to credit institutions, thereby falling within the scope of the exemption. However, in practice, careful assessment is still required based on the transaction structure and Member State regulators' interpretations and enforcement approaches.

5. Intra-group transactions

A third-country institution may be exempt when providing core banking services to its EU-based group entities[8].

Key Implementation Milestones for CRD 6

I. Before 10 January 2026: transposition into Member State law

Member States must transpose the Directive into domestic law. Based on progress to date, transposition has been uneven across Member States, and national implementing measures reflect differing regulatory approaches.

On 29 January 2026, German Federal Parliament took the lead and passed the "Banking Directive Implementation and Bureaucracy Reduction Act" (BRUBEG), amending the German Banking Act (Kreditwesengesetz, KWG) to transpose CRD 6. The amended German Banking Act largely follows CRD 6's approach on branch requirements.

Luxembourg's government submitted Bill No.8627 on 6 October 2025, which remains under committee review. The bill tends to emphasise a more relaxed stance under CRD 6 to maintain its attractiveness as a global financial hub. For example, it expressly provides that legacy contracts concluded before 11 July 2026 will not trigger branch requirements even if performed after that date.

The government of the Netherlands also submitted the "Capital Requirements Implementation Act 2026" (Implementatiewet kapitaalvereisten 2026) to the House of Representatives on 19 January 2026, and it is now under parliamentary review. The Netherlands leans toward a more prudent "phasing-out" approach for legacy contracts to reduce circumvention of the third-country branch requirements through contract renewals or amendments. The draft Act expressly states that legacy contracts

[6] Only after a third-country investment firm has completed ESMA registration (which involves an EU equivalence assessment of the third country's regulatory regime and the firm's ongoing compliance obligations) may it, without establishing any entity or TCB in the EU, provide MiFID investment services cross-border directly to professional clients and eligible counterparties as defined in Annex II, Section I of Directive 2014/65/EU. See Article 46(1) of Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012.

[7] See CRD 6, Article 21c.2.(b).

[8] See CRD 6, Article 21c.2.(c).

concluded before 11 July 2026 will generally no longer fall within the exemption if amended, renewed, or extended, thereby triggering branch requirements.

Ireland's Department of Finance conducted a public consultation in 2025 on transposition of CRD 6. Although the transposition deadline set out by CRD 6 has passed, Ireland has not yet published official domestic legislation or a draft bill as of now.

II. From 11 July 2026: expiry of exemption for legacy-contracts

After this date, newly signed core banking services contracts will no longer enjoy any form of legacy exemption. Any core banking services initiated thereafter must strictly comply with Article 21c.

For legacy contracts signed before 11 July 2026, any material changes made after that date (e.g., extensions, credit limit adjustments, key changes to interest rate benchmark) are highly likely to result in loss of exemption.

Therefore, the first half of 2026 will be a key window for Chinese banks to carry out reviews of their legacy contracts.

III. From 11 January 2027: full compliance

From 11 January 2027, all third-country banks carrying out business in the EU must comply with CRD 6 requirements for cross-border operations. Banks that fail to obtain the necessary branch authorisation or to operate through an EU subsidiary, may face penalties under CRD 6, including but not limited to administrative fines, public censure, and restrictions on senior management.

Impact of CRD 6 on Chinese Banks' EU Business

I. Structural challenges to operating models

1. Chinese banks without an EU legal entity

Previously, Chinese banks without an EU legal entity mainly relied on specific Member State exemptions to conduct offshore cross-border direct lending. For example, Germany's Federal Financial Supervisory Authority (BaFin) previously granted regulatory exemptions to certain third-country institutions that meet specific conditions under its domestic law, allowing them to provide cross-border financial services without obtaining a local license if conditions were met.

With CRD 6's implementation, Member States must adjust exemption arrangements that are inconsistent with the Directive. This means operating models that were previously permissible, or in regulatory grey areas, will need to transform. If such banks intend to continue providing core banking services to EU customers, unless they can prove they fall under strict exemptions such as reverse solicitation, they must establish a legally authorised EU subsidiary or branch.

2. Chinese banks already operating EU branches

The main impact of the Directive is a comprehensive upgrade of regulatory requirements: such banks will face stricter minimum requirements across capital adequacy, liquidity coverage, internal

governance, book-keeping, and more. For large Chinese banks with deeper EU footprints, this implies not just an increase in supervisory intensity, but also the need to allocate independent EU-based capital and liquidity coverage that align with the standard of Basel III.

Notably, if the total asset profile of the branches exceeds certain thresholds (e.g., total EU asset amount of the group reaching €40 billion or a single branch reaching €10 billion), regulators have the power to require conversion from a branch into a subsidiary to address potential systemic risk[9].

Additionally, some Member State regulators may also require existing branches to re-apply for authorisation to ensure compliance with CRD 6 and additional local requirements.

II. Analysis of the impact on the types of cross-border transactions conducted by Chinese banks

Under the CRD 6 regulatory framework, Chinese banks' EU transactions are facing higher local compliance requirements. Different product types face different compliance challenges because the underlying legal relationships and the risk-bearing parties differ. Set out below is our analysis of the impact of CRD 6 on several typical categories of cross-border services provided by Chinese banks:

1. Custody

CRD 6 compliance for custody depends on the purity of its function. If services are limited to technical or administrative support such as record-keeping and reporting, the risk of being classified as core banking services is relatively low.

However, once the custody arrangement is tightly linked to credit limits, performance guarantees, or liquidity support agreements, we consider that its legal nature may change fundamentally, and regulators may view it as a disguised form of core banking services.

For Chinese banks, the key to compliance lies in building robust "firewalls", clearly separating custody asset management activities from the bank's assumption of risk. In particular, if a Chinese bank provides EU customers with custody solutions that include financing features, it should be alert to the risk that the arrangement may be "looked through" and characterised as the provision of core banking services.

2. Guarantees and standby letters of credit

Due to their clear credit-substitution features, guarantees, standby letters of credit (SBLCs), and credit commitment letters are very likely to be directly classified as core banking services.

A common scenario in practice is that a Chinese bank may enhance the credit of a borrower in the EU by issuing an SBLC, with an EU local bank providing the underlying loan. In this structure, as the loan itself is provided by an EU local bank, the compliance risk is relatively low. However, the credit enhancement arrangement constitutes "guarantees and commitments" under the CRD 6 regime. If the Chinese bank issuing the SBLC has no establishment in the EU, and the issuance is viewed as a systematic service providing to EU customers, the guarantee or commitment may itself be

[9] See CRD 6, Recital (21).

characterised as non-compliant.

Accordingly, Chinese banks should consider alternative approaches as soon as practicable. For Chinese banks that already operate branches in the EU, one option is to migrate their operation so that the SBLCs are issued by an EU subsidiary or EU branch. For Chinese banks with no presence in the EU, they may explore whether the transaction can be implemented through cooperation with local banks.

3. Risk participation

In this structure, a bank located in the EU, acting as the lead bank, signs a loan agreement with the borrower and disburses the funds directly. The Chinese bank, as a participating bank, assumes all or part of the credit risk by entering into a risk participation agreement with the lead bank.

Where the Chinese bank participates on a funded basis by advancing funds to the lead bank, the structure avoids a direct contractual relationship with the borrower in form. However, under CRD 6, it should be noted that if the Chinese bank is deeply involved, particularly where risk and return are fully transferred, its involvement may still be characterised as a substantive provision of services into the EU.

A risk participation (unfunded) structure is closer to a credit default swap. Once an advance payment or indemnity is triggered, the substance of the legal relationship may be traced back to the category of "guarantees and commitments", and may therefore remain subject to Article 21c.

4. Syndicated loans

In syndicated lending transactions, a bank's compliance risk exposure can vary significantly depending on the role it plays.

The lead arranger role is the most likely to be characterised as a substantive provision of services into the EU. Even if the loan agreement is governed by English law and the funding flows and settlement are completed in London, where the borrower is an EU entity and the Chinese bank, as an initial lender, signs the agreement directly and commits a credit limit to the borrower, regulators are likely to view the bank as providing core banking services to the EU market. In addition, as the lead arranger is responsible for early-stage due diligence, term negotiations and syndication, these activities may be viewed as involving elements of active marketing. Even if the borrower has nominally initiated the transaction, the complexity of arranging a syndicate typically goes well beyond the passive boundaries of reverse solicitation. In principle, from 2027 onwards, Chinese banks are not recommended to continue acting as lead arrangers or initial lenders for EU borrowers.

If the Chinese bank participates only as an ordinary syndicate lender, risk exposure is narrower but compliance risk remains. A cautious approach is therefore recommended during the transitional period up to July 2026. The reason is that, as an ordinary syndicate lender, the Chinese bank remains a party to the facility agreement and holds contractual claims directly against the EU borrower and therefore may still fall within the scope of Article 21c.

5. Aircraft project financing

In aviation finance, a long-established mainstream structure is for an Ireland-incorporated SPV to act as lessor, hold the aircraft assets and seek a cross-border loan from an onshore Chinese bank or its non-EU branch (e.g., the London branch). However, with the implementation of CRD 6, the structure of cross-border direct lending as such is likely to come under closer compliance scrutiny.

The core challenge lies in the borrower's jurisdictional nexus (i.e., the Irish SPV). Under the "look-through" approach of Article 21c, where the borrowing entity is located in an EU Member State, granting credit to it is highly likely to be characterised as the provision of core banking services in that Member State.

Some banks may attempt to rely on the reverse-solicitation exemption as a safe harbour, arguing that the financing request was initiated by the Irish SPV. In practice, however, where an Irish SPV repeatedly and systematically seeks financing from the same Chinese bank, regulators are unlikely to accept that the approach was genuinely ad hoc, and may instead be inclined to characterise it as the bank carrying out core banking services in Ireland.

As a global hub for aircraft leasing, it remains uncertain whether Ireland will adopt more flexible supporting policies or implementing guidance for specific sectors such as aviation finance. It is therefore advisable to closely monitor Irish legislative and regulatory developments and to build sufficient flexibility into post-2026 new financing projects to accommodate potential policy adjustments.

Chinese Banks' Path Forward: Compliance-Driven Strategic Transformation

As July 2026 approaches, Chinese banks' EU business has entered a critical phase of proactive reshaping. Banks currently providing cross-border direct lending to EU Member States should systematically assess their status and implement measures promptly to ensure continuity and compliance.

I. Review legacy business

Chinese banks should immediately begin an EU-wide review of legacy contracts, especially long-tenor credit contracts that remain outstanding after 11 July 2026 and may face material changes such as tenor extensions or interest rate adjustments etc. For legacy business that are highly likely not exempt, banks may consider confirming a pathway for transferring the relevant exposures in the first half of 2026 (e.g., via novation agreements, risk participation, or direct asset sales) so that, before CRD 6 becomes fully applicable from January 2027, the relevant exposures can be transferred to an appropriately licensed entity established within the EU.

II. Reassess EU footprint

Facing the compliance impact of CRD 6, Chinese banks that have not yet established a presence in the EU should, in light of their potential growth and footprint, carefully weigh the option of establishing an EU subsidiary against setting up a third-country branch. Establishing a subsidiary means that, once authorised in a single Member State, the bank can benefit from "passporting" rights. Through this right, the bank may use that Member State as a base to provide banking services across the EU.

By contrast, authorisation for a third-country branch is typically subject to strict territorial limitations and, in principle, is limited to conducting business in the Member State where the branch is established. For banks seeking to expand their businesses across multiple EU jurisdictions, third-country branches are therefore clearly less flexible.

For Chinese banks that have already made an initial EU entry, the compliance balance is increasingly tilting towards the higher-cost end. Even existing third-country branches will face materially more intensive regulation and higher compliance requirement under CRD 6, and in some respects the regulatory burden may begin to converge with that applicable to subsidiaries.

Given this fundamental shift in the regulatory "red line", relevant financial institutions should reassess their EU operating structure from a strategic perspective. Chinese banks should not treat CRD 6 merely as a one-off compliance "gap-filling" exercise, but they should take the opportunity to prudently evaluate whether their existing legal-entity structure remains fit for purpose.

III. Prudently assess exemptions

Although Article 21c blocks most cross-border "direct access" paths, CRD 6 retains a small number of exemptions. Chinese banks must conduct a highly granular, look-through compliance assessment to avoid inadvertently crossing regulatory "tripwires".

Under CRD 6, where a financial service genuinely arises from the client's exclusive initiative, the bank may be exempt from the requirement to obtain a local licence. In regulatory practice, however, EU authorities are expected to apply an almost stringent standard when assessing this pathway. For Chinese banks pursuing scalable and systematic expansion, reliance on reverse solicitation not only shifts the burden of proof onto the bank (to prove it was entirely passive), but it also lacks commercial scalability due to its inherent constraints on proactive client acquisition. Accordingly, reverse solicitation can only serve as a supplementary solution for occasional transactions, and should not be treated as a sustainable operating model. By contrast, transactions with EU-authorised peer institutions or with entities within the same group are more operationally feasible. However, even these structures may attract secondary risk of being accused of "regulatory arbitrage" under a look-through regulation.

Given the complexity of exemption analysis, Chinese banks should, during this period of strategic transition, engage specialist legal counsel with a cross-border regulatory perspective to provide robust legal opinions on specific transaction structures. This helps to ensure the legal effectiveness of the chosen structures and, in the event of regulatory scrutiny, serves as key evidence that the bank has discharged its duty of prudent due diligence.

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	**Hanmeng LI**	**Attorney-at-law**
	Tel:	+86 898 3665 5003
	Email:	hanmeng.li@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:	+1 516 960 2071
	Email:	mike.chiang@hankunlaw.com
Silicon Valley	**Melody HE**	**Attorney-at-law**
	Tel:	+852 2820 5686
	Email:	melody.he@hankunlaw.com