

合规警报

本栏目还包括：
Also in this section:

82 中国企业对日投资的路径选择
Overview of Chinese investment in Japan

84 瑞士法的“虚假自雇”概念
“Fictitious self-employment” in Switzerland



COMPLIANCE ALERTS

在全球业务运营中，中国企业如何应对与日俱增的美国监管力度？

HOW SHOULD CHINESE COMPANIES FACE INCREASED
US ENFORCEMENT RISK FROM THEIR GLOBAL BUSINESS OPERATIONS?

近

期美国与俄罗斯、朝鲜和伊朗之间的紧张局势日趋升级，已促使特朗普政府针对这些国家及与之存在商业往来或为其提供支持的企业和金融机构采取新的制裁行动、进行额外出口管制并实行新的反洗钱措施。

虽然美国这些措施的政策目标尚未明确包括对中国进行经济制裁，但这些行动已对许多中国企业和金融机构产生了重要的间接影响。事实上，在过去一年中，美国对中国实体施加了严苛的制裁，对中国企业处以巨额罚款，将一些中国银行与美国金融系统的往来完全切断。新颁布的制裁规定意味着，美国将对与朝鲜、俄罗斯和伊朗存在某些类型商业往来的中国企业采取类似措施。这些国际执法风险方面的发展趋势突显出中国企业理解美国法律的重要性，否则会承担严重的后果。

针对中国企业的执法

特朗普政府已采用各类政策工具处罚违反美国法律、支持与美国关系紧张的外国政府的中国企业。

一、经济制裁。2017年6月，美国财政部海外资产控制办公室（OFAC）将两名中国公民列入《特别指定国民和禁止往来人员名单》（《SDN名单》），因为OFAC认为此二人为受制裁的朝鲜实体经营幌子公司。同时，OFAC还指出大连宁联船务有限公司涉嫌违反联合国贸易禁令，向朝鲜走私奢侈品。

2017年11月，在特朗普政府将朝鲜列为支持恐怖主义国家之后，OFAC随即将与朝鲜有长期商业往来的四家中国企业和一名中国个人列入《SDN名单》，理由为他们从事面向朝鲜的重要货物进出口，包括与建设核反应堆有关的计算机、机械和原材料。

二、反洗钱专项措施。2017年6月，美国财政部金融犯罪执法网络（FinCEN）建议将中国丹东银行列为“存在重要洗钱问题”的银行。FinCEN指称，丹东银行在2012年5月至2015年5月之间通过其美国代理银行账户处理了逾25亿美元的交易，是朝鲜进入美国和国际金融体系的“管道”。FinCEN称其中一些资金被用于代表参与朝鲜大规模杀伤性武器和弹道导弹计划的企业促进数百万美元的交易。FinCEN于2017年11月发布了执行这些专项措施的最终裁决，届时丹东银行与美国金融系统的往来实际上完全切断。

三、筑坝搜索票。美国政府还利用所谓的“筑坝搜索票”（damming warrants）扣押代表朝鲜行事的中国企业的资金。当对账户设置筑坝搜索票时，美国政府禁止该账户的所有资金流出，并扣押在搜索票期限内流入账户的任何资金。2017年早些时候，哥伦比亚特区一家联邦地区法院授予美国司法部申请的对八家美国金融机构代理银行账户设置的筑坝搜索票，这八家金融机构被指由中国企业利用，代表朝鲜处理了数千万美元。在筑坝搜索票有效期间，司法部最终扣押了经由代理银行账户的逾400万美元资金。

四、多机构联合执法行动。美国政府已针对违反制裁规定和出口管制法的企业采取了行动。在近期一次著名的执法行动中，中国的电信公司中兴通讯股份有限公司承认违反《国际紧急状态经济权力法》，并同时与OFAC、美国司法部和美国工业安全局（BIS）就中兴故意逃避美

The recent escalation of tensions between the US and Russia, North Korea and Iran has triggered the Trump administration to unveil new sanctions, implement additional export controls, and impose novel anti-money laundering measures directed at these countries – as well as companies and financial institutions that do business with or otherwise support those jurisdictions.

While the US' stated policy goals for these measures have not included imposing economic pain on China, these actions have had important indirect consequences for many Chinese companies and financial institutions. During the past year, the US has targeted Chinese entities with severe sanctions, slapped massive fines on Chinese firms, and wholly cut off certain Chinese banks from the US financial system.

Newly enacted sanctions suggest the US will take similar action against Chinese firms that carry out certain types of business with North Korea, Russia and Iran. These developments in international risk enforcement underscore why it is important for Chinese firms to understand US law, as well as the severe and negative consequences that can flow to Chinese companies that fail to do so.

ENFORCEMENT DIRECTED AT CHINESE COMPANIES

The Trump administration has utilized a variety of policy tools to punish Chinese firms that violate US law, or that support foreign governments that have strained relations with the US.

1. Economic sanctions. In June 2017, the US Department of Treasury's Office of Foreign Assets Control (OFAC) added two Chinese citizens to its Specially Designated Nationals and Blocked Persons List (SDN List) because the OFAC determined these individuals were operating front companies for sanctioned North Korean entities. Contemporaneously, the OFAC also designated Dalian Global Unity Shipping, purportedly for smuggling luxury goods into North Korea in violation of a UN ban on such trade.

In November 2017, immediately after the Trump administration classified North Korea as a state sponsor of terrorism, the OFAC designated four Chinese companies and a Chinese individual with longstanding commercial ties to North Korea for engaging in significant importation and exportation activities to and from North Korea, including computers, machinery and raw materials associated with the construction of nuclear reactors.

2. Anti-money laundering special measures. In June 2017, the Financial Crimes Enforcement Network (FinCEN), another office within the Treasury Department, proposed to designate the Chinese Bank of Dandong as a “primary money laundering concern”. FinCEN asserted that the Bank of Dandong served as a “conduit” for North Korea to access the US and international financial systems, by processing more than US\$2.5 billion in transactions through its US correspondent accounts between May 2012 and May 2015.

Some of these funds were used to facilitate millions of dollars of transactions on behalf of companies involved in North Korea's weapons of mass destruction and ballistic missile programmes. When FinCEN issued a final rule last November implementing these special measures, the Bank of Dandong was effectively cut off from the US financial system.



国制裁规定和出口管制法, 以及使用原产于美国的设备和软件建设、运营和服务伊朗电信设施的指控达成和解协议。中兴同意支付总计 8.92 亿美元和解其潜在责任, 其中 OFAC 从中收取超过 1 亿美元罚款。这是 OFAC 有史以来对非金融机构进行的最大规模民事处罚。

此外, 多家媒体报道称, 美国政府已启动类似的大范围调查, 评估华为技术有限公司遵守美国制裁规定和出口管制的情况。据报道, OFAC 和 BIS 均已向华为发出传票, 要求其提供以往对古巴、伊朗、朝鲜、苏丹和叙利亚的出口信息。这些传票表明华为可能与中兴一样, 违反美国法律向这些国家输出过产品或技术。

五、刑事控告。违反美国制裁规定和反洗钱法的中国企业还可能面临刑事指控。事实上, 美国司法部经常同 OFAC 合作, 对试图逃避美国制裁的外国国民进行刑事立案。2016 年 8 月, 司法部指控中国贸易公司丹东鸿祥实业发展有限公司连同四名公司高管违反美国联邦法, 利用在境外司法管辖区设立的幌子公司协助一家受制裁的朝鲜公司逃避美国制裁。司法部还针对丹东鸿祥在二十五家中国银行的资金提起了民事没收诉讼, 理由是这些资金涉嫌洗钱。在司法部诉讼进行的同时, 丹东鸿祥实业发展有限公司及其高管人员因其有关行为被 OFAC 列入《SDN 名单》。

近期制裁立法

在过去一年中, 新的立法和政策发展表明, 美国政府意图制裁继续与俄罗斯和朝鲜开展商业活动的其他中国企业。

一、《以制裁反击美国敌人法案》。2017 年 8 月, 特朗普总统签署《以制裁反击美国敌人法案》。《法案》给予美国财政部广泛授权, 扩大对与俄罗斯和朝鲜开展业务的外国实体和个人的二级制裁。

3. Damming warrants. The US government has also utilized so-called “damming warrants” to seize funds of Chinese firms acting on behalf of North Korea. When a damming warrant is placed on an account, the US government prevents all funds from exiting the account and seizes any funds that flow into the account during the pendency of the warrant.

In early 2017, a federal district court in the District of Columbia granted the Department of Justice’s (DOJ) application to attach damming warrants for correspondent accounts at eight US financial institutions that allegedly were used by Chinese firms to process tens of millions of dollars on behalf of North Korea. The DOJ ultimately seized more than US\$4 million in funds routed through the correspondent accounts while the damming warrants were in place.

4. Multi-agency enforcement actions. The US government has targeted Chinese companies for violating sanctions and export control laws. In one notable recent enforcement action, the China-based telecommunications company Zhongxing Telecommunications Equipment Corporation (ZTE) pleaded guilty to violating the International Emergency Economic Powers Act and simultaneously entered into settlement agreements with the OFAC, the Department of Justice, and the Bureau of Industry and Security (BIS) related to allegations that it had wilfully evaded US sanctions and export control laws by building, operating and servicing telecommunications in Iran using US-origin equipment and software. ZTE agreed to pay US\$892 million to resolve its potential liability, with the OFAC collecting more than US\$100 million. This penalty is the largest civil penalty that the OFAC has ever imposed on a non-financial institution.

In addition, various media reports indicate that the US government has opened a similarly wide-ranging investigation to assess telecommunications equipment and service company Huawei Technologies’ compliance with US sanctions and export controls. Both the OFAC and the BIS reportedly have issued subpoenas to Huawei demanding that it turn over information regarding its historical exports to Cuba, Iran, North Korea, Sudan and Syria. Such subpoenas would suggest that Huawei, like ZTE, also may have shipped products or technology to those countries in contravention of US law.

5. Criminal prosecutions. Chinese firms that violate US sanctions and anti-money laundering laws can face criminal charges. In fact, the DOJ and the OFAC frequently collaborate on building criminal cases against foreign nationals who attempt to evade US sanctions.

In August 2016, the DOJ charged a Chinese trading company, Dandong Hongxiang Industrial Development, along with four company executives, with violating US federal law by using front companies established in offshore jurisdictions to assist a sanctioned North Korean company in evading US sanctions.

The DOJ also initiated a civil forfeiture action against Dandong Hongxiang’s funds in 25 Chinese banks on the basis that those funds were implicated in a money laundering scheme. In parallel with the DOJ actions, the OFAC added Dandong Hongxiang Industrial Development and its executives to the SDN List for their conduct.

RECENT SANCTIONS LEGISLATION

In the past year, new legislative and policy developments indicate that the US government intends to sanction additional Chinese

[美国制裁、出口管制和反洗钱法律] 的范围和适用性并不总是直观清晰, 而是能以出人意料的方式适用于中国企业

The scope and application of [US sanctions, export controls, and anti-money laundering laws] is not always intuitive, and they can apply to Chinese companies in unexpected ways

该《法案》要求特朗普总统对故意向俄罗斯深水项目、北极海上项目或页岩油项目进行大量投资或提供财务支持的外国实体施加各种二级制裁。此外, 对于代表美国制裁名单中的俄罗斯人士疏通重大交易的外国人士, 总统有义务将其纳入《SDN 名单》。

类似地, 该《法案》还授权特朗普总统制裁故意与朝鲜开展某些交易的外国国民, 包括代表任何朝鲜金融机构维持代理银行账户的人士(联合国安理会特别批准的除外), 以及从朝鲜进出口任何防御物品或防御服务的人士。《法案》还要求特朗普总统制裁使用朝鲜劳动力的外国人士, 除非与工作条件和工资使用情况有关的特定条件得到满足。

鉴于中国与俄罗斯和朝鲜的历史经济关系, 这一立法很可能向中国企业和金融机构提出特殊挑战。

二、新的朝鲜制裁。在上述《法案》成为法律后不久, 特朗普总统对朝鲜施加了更广泛的制裁。这些新的制裁措施授权 OFAC 对朝鲜国民以及与朝鲜有业务往来的外国企业和银行施加制裁。最值得注意的是, 对于已与朝鲜从事重要跨境商业交易的外国实体而言, 即便这些交易与朝鲜的核计划或弹道导弹计划无关, 上述制裁规定也允许 OFAC 冻结该等外国实体的资产。此外, 向朝鲜提供银行服务的外国金融机构可能会被冻结资产或丧失其进入美国金融系统的通路。

根据适用方式, 上述制裁规定可能代表着美国制裁政策的重要转变。历史上, 考虑到对美国投资者和全球金融体系的潜在附带后果, 美国一直不愿针对大型中国

companies that continue to engage in commercial activities with Russia and North Korea.

1. Countering America's Adversaries Through Sanctions Act. In August 2017, US President Donald Trump signed into law the Countering America's Adversaries Through Sanctions Act. The act granted the Department of Treasury broad authority to expand secondary sanctions against foreign entities and individuals that conduct business with Russia and North Korea.

The act requires President Trump to impose various secondary sanctions on foreign entities that knowingly make a significant investment in, or provide financial support for, Russian deepwater, Arctic offshore or shale oil projects. In addition, the president is obliged to designate foreign persons for inclusion on the SDN List who facilitate significant transactions on behalf of Russian persons targeted by US list-based sanctions.

Similarly, the act mandates President Trump to designate foreign nationals who knowingly engage in certain dealings with North Korea, including maintaining a correspondent banking account on behalf of any North Korean financial institution (except as specifically approved by the UN Security Council), and importing to or from North Korea any defence articles or defence services. President Trump also must designate foreign persons that utilize North Korean labourers unless specific conditions relating to working conditions and the use of wages are met.

Given China's historical economic ties with Russia and North Korea, this legislation is likely to present particular challenges to Chinese companies and financial institutions.

2. New North Korea sanctions. Shortly after the act became law, President Trump imposed another broad set of sanctions on North Korea. These new sanctions authorize the OFAC to sanction North Korean nationals, as well as foreign companies and banks that do business with North Korea. Most notably, these sanctions permit the OFAC to freeze the assets of foreign entities that have engaged in significant cross-border, commercial transactions with North Korea – even if such transactions are unrelated to North Korea's nuclear or ballistic missile programme. In addition, foreign financial institutions providing banking services to North Korea could be subject to asset freezes or lose their access to the US financial system.

Depending on how they are applied, these sanctions could represent a major shift in the US sanctions policy. Historically, the US has been reluctant to target large Chinese companies and major Chinese financial institutions because of the potential collateral consequences for US investors and the global financial system.

However, the sweep of these sanctions measures may signal that the US is increasingly willing to sanction large Chinese companies and banks that continue to engage in significant commercial dealings with North Korea, irrespective of any potential global impact.

企业和主要中国金融机构采取行动。不过，这些新的制裁措施的彻底性可能释放着一种信号：美国越来越愿意制裁那些继续与朝鲜开展重要商业交易的大型中国企业和银行，而不顾潜在的全球影响。

中国企业的主要应对措施。我们建议中国企业和金融机构采取以下措施评估其面临美国制裁、出口管制和反洗钱执法的潜在风险：

- 了解美国法律制度。中国企业和银行应认真了解美国制裁、出口管制和反洗钱法律。这些法律的范围和适用性并不总是直观清晰，而是能以出人意料的方式适用于中国企业。中国企业应投入精力，研究和理解这些监管制度，较好地识别风险领域，并可以改变行为方式，降低风险。相反，不了解美国法律如何运作、如何适用，则可能面临巨额责任。
- 审查与伊朗、朝鲜和俄罗斯的交易。美国寻求通过经济制裁、出口管制和反洗钱法推动实现其国家安全目标。伊朗、朝鲜和俄罗斯是目前对美国的最大威胁，美国政府已针对这些国家实施了广泛的法律措施。中国企业应对其与这些国家开展的交易进行评估并分类，然后基于可能的执法风险判断与这些国家继续保持互动是否明智。
- 评估全球合规风险环境。最后，中国企业应对其与美国以及美国商业和金融机构的联系进行评估，判断其在美国法项下可能面临的风险。一个企业的风险环境将涉及多个因素，包括其是否开展全球运营，是否参与跨境交易，是否从事可用于军用的源部件或终端产品的交易。此外，中国企业所在的行业领域也关系重大。在美国法下没有哪两家企业会遇到相同的风险，因此企业了解自身特殊的风险环境至关重要。

结论

过去的一年表明了中国企业因违反美国法律或与朝鲜等受制裁国家开展交易而可能面临的后果。新的制裁规定表明，美国政府日后将继续针对中国企业采取行动。鉴于美国执法工作范围的扩大，以及美国针对中国传统盟友和贸易伙伴的国家安全目标，中国企业和金融机构深入理解其在这种变幻莫测的风险环境中的潜在风险将大有裨益。▲

Michael Casey 是凯易律师事务所伦敦办公室合伙人，Cori Lable 是凯易香港合伙人，张天镜是凯易上海合伙人。凯易香港办公室律师宁宁对本文亦有贡献。

Michael Casey is a London-based partner, Cori Lable is a Hong Kong-based partner, and Tiana Zhang is a Shanghai-based partner at the international law firm Kirkland & Ellis. Ning Ning, Kirkland & Ellis' associate in Hong Kong, also contributed to this article.

3. Key takeaways for Chinese firms. We recommend that Chinese firms and financial institutions take the following measures to evaluate their potential exposure to US sanctions, export controls, and anti-money laundering enforcement:

- Understand the US legal regime. Chinese companies and banks should endeavour to understand US sanctions, export controls, and anti-money laundering laws. The scope and application of these laws and rules is not always intuitive, and they can apply to Chinese companies in unexpected ways. Chinese firms that invest the effort to review and understand these regulatory regimes will be well positioned to identify risk areas and potentially alter their conduct to mitigate those risks. In contrast, failing to understand how US laws operate and are applied can lead to significant liability.
- Scrutinize dealings with Iran, North Korea, and Russia. The US seeks to advance its national security objectives through economic sanctions, export controls and anti-money laundering laws. Iran, North Korea and Russia are the nations that currently pose the greatest threat to America, and the US government has implemented wide-ranging legal measures related to these countries. Chinese companies should assess and catalogue what types of dealings they have with these countries, and then evaluate whether continued interactions with such countries make sense in light of the applicable enforcement risk.
- Assess global compliance risk profile. Finally, Chinese companies should assess their nexus to the US and American businesses and financial institutions to determine what risk they may face under US law. A firm's risk profile will turn on a number of factors, including whether it operates internationally, participates in cross-border transactions, and deals in source components or end products that could have a military application. In addition, the industrial sector in which a Chinese company functions can also be relevant. No two companies will encounter the same risks under US law, so it is important for companies to understand their specific risk profile.

CONCLUSION

The past year has illustrated the consequences that Chinese companies may face for violating US law or transacting business with sanctioned jurisdictions such as North Korea, and new sanctions suggest that the US government will continue to target Chinese companies in the future.

In light of the increased scope of US enforcement efforts, and specific US national security objectives targeting traditional allies and trade partners of China, Chinese firms and financial institutions would be well served to understand their potential exposure under this rapidly changing risk landscape. ▲