

VIETNAM

Vietnam must strengthen criminal laws against trade secret theft

Tilleke & Gibbins



Tu Anh Tran and Duc Anh Tran

In today's knowledge-driven, constantly connected global economy, a comprehensive legal environment is necessary to deter and address the theft of intellectual property, especially vulnerable IP assets like trade secrets.

Trade secrets can give companies a competitive edge, and are obvious targets for misappropriation. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which took effect in Vietnam on January 14 2019, has set a floor for its members to establish criminal sanctions for trade secret misappropriation. Vietnam's compliance with the CPTPP's requirements is necessary to ensure a healthy business environment as the country continues its path of economic integration.

Trade secret crimes under the CPTPP and Vietnam's Criminal Code

Article 18.78 of the CPTPP requires its signatories to provide criminal procedures and penalties for one or more of the following:

- Unauthorised and willful access to a trade secret held in a computer system;
- Unauthorised and willful misappropriation of a trade secret, including by means of a computer system; or
- Fraudulent disclosure, or unauthorised and willful disclosure, of a trade secret, including by means of a computer system.

Vietnam's Criminal Code 2015 (as amended in 2017) does not explicitly stipulate any trade secret crimes. However, the articles below might apply to some degree to trade secret misappropriation:

- Article 159. Infringement of secrecy or security of another person's mail, telephone, telegraph or other form of private information exchange;
- Article 288. Illegal provision or use of information on computer networks or telecommunications networks; and
- Article 289. Illegal infiltration into another person's computer network or telecommunications network or electronic device.

One could argue that these articles of the Criminal Code, which mainly deal with the unlawful acquisition of information held in a computer network, suffice to meet the CPTPP's requirements. However, their scope is limited to information exchange, information on computer networks, etc. and only covers a modest portion of all 'trade secrets', which, as broadly defined in Vietnam's IP Law, encompass all types of information related to business that are commercially valuable, except for those related to personal identification, state management, and national defense and security.

These articles are principally designed to address misconduct related to private personal information (which may be unrelated to business) via computer systems. The law lacks any criminal measures to tackle 'offline' misappropriation, let alone trade secret theft or economic espionage. Many instances of trade secret misappropriation still occur through traditional channels that are paper-based, not digital. As a trade secret can simply be in the form of a written note containing 'tricks of the trade', prying eyes can steal the secret at a glance.

One of the biggest threats to trade secret preservation is employees who break the promise of confidence by carrying a company's precious business secrets to third parties. In a recent case in Vietnam, a reputable security software company found that an infringer (suspected to be a former employee) was offering source code from the company's software (protectable as

a trade secret) for sale on the internet. This type of insider threat clearly exists even in the most well-secured entity, and could result in severe economic losses and reputation damage if not properly safeguarded.

Outlook

Criminal prosecution is considered the strongest method of deterring IP crime. Yet for crimes related to trade secrets, the criminal sanctions in Vietnam do not provide enough of a deterrent, or sufficient means of trade secret protection as mandated by the CPTPP. Competitors in cut-throat competition can reap the benefit of others' trade secrets without bearing the costs or risks of investing in their own R&D, knowing that any punishment will likely be minimal.

To our knowledge, only three cases related to trade secrets have been handled by Vietnamese authorities:

- A 2005 case handled by the People's Court of Ho Chi Minh City concerning the dismissal of an employee for violating internal labor rules on confidentiality;
- A 2010 case handled by the People's Court of Duc Hoa District, Long An Province, concerning the alleged violation of a non-compete clause affecting trade secrets; and
- An administrative case regarding trade secrets currently being handled by the Inspectorate of the Ministry of Science and Technology.

No criminal sanctions have yet been issued by the Vietnamese authorities for trade secret crimes.

With the current gaps in the scope of the criminal regime for trade secrets, it does not appear that a patchwork of other laws can cover the emerging threats, especially when the Vietnamese economy is opening a wide door to embrace the latest tastes and trends of integration.

Supplementing the current legal framework with strong criminal provisions on trade secrets, in har-

monisation with the CPTPP, will help Vietnamese businesses, particularly SMEs, to thrive and gain the upper hand in dealing with piracy risks, and also help foreign enterprises prevent the erosion of their competitive edge, promising a bright future for Vietnam in attracting both domestic and foreign investment.