

# Minimizing Headaches During China Investigations

September 7, 2016

Anti-corruption

---

By Eric Carlson

Any company with a more than a small presence in China is likely to need to conduct an internal investigation in China at some point. While investigations in China are not wholly different than in other jurisdictions, our experience handling scores of such investigations leads us to the conclusion that companies can take certain steps in advance to minimize headaches if and when such an investigation in China is needed.

## Properly Adopt Company Policies Under PRC Law

---

Most companies have a global code of conduct and likely a global anti-corruption policy that applies to employees in China. A company may not realize that in order for the policies to be effective under PRC law, they need to be provided to the trade union (if one exists) or to all local employees for review, discussion, and comment. Failure to do so (or failure to provide these policies in Chinese) materially increases the risk that employees may challenge or seek to invalidate these policies as being inapplicable, particularly in cases of termination of employment based on serious violations of company policy.

## Include Privacy Provisions in Contracts and Notices

---

Collecting electronic data from employees' IT assets is often needed in the initial stages of an investigation. PRC privacy laws have evolved quickly in recent years. Employers are required to keep employee data confidential, and should obtain advance consent prior to sharing such information outside of the company. In view of such a requirement, companies can best protect themselves and mitigate risk by:

- Implementing an IT use policy stating that the company has the right to access, monitor, review, and disclose to third parties information on company-owned IT assets. It is important to ensure that the policy is available in Chinese and to adopt the policy pursuant to the PRC Labor Contract Law.
- Having each employee acknowledge receipt and, if possible, acceptance of the policy by signing a hard-copy document or via electronic means. Ideally, the acknowledgment should be in Chinese or the working language used by the employee to avoid any confusion or future dispute with respect to the content of the policy.

- Placing prominent notices (in Chinese and any other working language) around the workplace and/or online (for example, displaying it as a customized legal notice or start-up message when employees log in to company computers or networks) that reminds employees of the policy.
- Including provisions in employment contracts referencing the policy and the company's rights over company-owned IT assets.

## **Conduct a Front-End State Secrets Analysis**

---

The PRC Law on Protecting State Secrets -- an often misunderstood law -- broadly prohibits unauthorized individuals and entities from acquiring, possessing, recording, storing, or transferring outside of China information deemed to be a "state secret." For many -- perhaps most -- multinational companies, the law will not significantly impair an investigation in China or require additional steps. However, in some cases, state secrets may be post more significant risks that will need to be navigated. In most cases, these risks can be analyzed in advance -- before an investigation arises -- working with a China-based lawyer who has experience with both China investigations and state secrets issues. The analysis usually turns on factors such as the industry, whether the Chinese affiliate has sales to or is in a joint venture with a government or state-owned entity, and what information the Chinese affiliate has access to.

Conducting this front-end analysis can often spare significant handwringing in the early days of an investigation when decisions need to be made about how to structure (or restructure) an investigation to account for potential state secrets sensitivities.

## **Conduct an Assessment of China-Based IT Architecture and Access**

---

In our experience, the key early days of a fast-moving investigation are often spent tracking down IT-related questions such as:

- where email servers are located that serve emails for China-based custodians;
- what shared or network drives are accessible to certain China employees;
- whether China-based employees have company-issued phones, or have company email access from their personal devices;
- what remote access to laptops can be obtained from headquarters versus locally in China;
- what kind of images can be made by company IT systems;
- whether instant messaging software is used in China, and whether those messages are preserved and accessible;
- whether disaster recovery systems (e.g., back-up tapes) are in place; and
- what accounting systems are used in China, and what transaction data and details are accessible locally and remotely.

Most of these questions can be assessed in advance and updated periodically (e.g., in an IT system map), rather than losing precious time after an allegation arrives.

## **Institute or Update a Dawn Raid Protocol**

---

Particularly for companies in sectors likely to be visited by PRC regulatory authorities, consider implementing a protocol on best practices to respond to such visits. Companies are increasingly training both reception staff and local or regional legal personnel on how to appropriately handle such visits, such as assigning a designated liaison, documenting requests and interviews, and monitoring documents or other items copied or taken by authorities.

## **Understand PRC Laws on Bribery and Corruption, Particularly Commercial Bribery**

---

At a conceptual level, the contours of PRC laws on bribery and corruption significantly overlap that of other corruption statutes, such as the FCPA and UK Bribery Act. But some differences exist -- PRC law, for instance, has no exception for facilitating payments and very few (and different) affirmative defenses or exceptions. More broadly, PRC law provides for both administrative and criminal penalties for commercial bribery. Local enforcement authorities have significant enforcement discretion, so it may not be in a company's best interest to assume that because an improper payment was to a purely private individual, it not need be investigated or does not pose significant legal risk (setting aside if there are books and records or internal control issues that may create liability under the FCPA).

## **Realize that US-Style Legal Privileges and Immunities Do Not Exist in China**

---

The attorney-client privilege and the work product doctrine do not exist under PRC law. China-based attorneys (both in-house and sometimes external counsel) may not be aware of the importance of these privileges and immunities and the need to structure and execute investigations in a way to maximize the protections of these privileges and immunities outside of China, even if they do not apply inside of China. For this reason, we recently drafted an article in English and Chinese (available from the authors upon request) about how to preserve privilege when conducting an internal investigation in China.

## **Understand PRC Laws Related to Whistleblowers and Whistleblower Protection**

---

While many allegations in China come from anonymous sources, where the source is known, ensure that allegations are handled in a way to avoid missteps that could be construed as retaliation.

## **Understand PRC Laws on Discipline and Termination and Associated Requirements and Evidentiary Standards**

---

PRC laws related to employee discipline and termination are somewhat different than in other countries, particularly the United States. Labor tribunals that hear employment complaints and suits are widely perceived to be pro-employee, and written evidence carries far more weight than oral testimony. Companies should collect sufficient evidence -- and in a forensically sound way -- during an investigation to mitigate the risk that an employee terminated for conduct identified during an investigation later has strong grounds for a wrongful termination suit.

## **Identify Local Resources**

---

Many investigations will require local assistance -- internal and external. Internal resources may include IT managers to assist with preservation efforts or accounting managers to identify transactions of interest, in addition to local legal, compliance, audit, and management staff. External resources may involve forensic accounting firms, forensic technology firms, law firms, private investigative firms, and translation vendors. Having a short list of recommended or preferred vendors in these areas that have significant experience handling investigations in China can save valuable time in the early days of a fast-moving investigation.

\* \* \* \*

This article first appeared as a two-part series on the FCPA Blog. The original posts can be viewed [here](#) and [here](#). [Eric Carlson](#), a contributing editor of the FCPA Blog, is a Shanghai-based partner at Covington & Burling LLP specializing in anti-corruption investigations and compliance, with a particular focus on China. He speaks fluent Mandarin and Cantonese and can be contacted [here](#).

## Anti-corruption

If you have any questions concerning the material discussed in this document, please contact any of the following senior members of our Global Anti-Corruption Practice Group:

Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Tammy Albarrán	+1 415 591 7066	talbarran@cov.com
Stephen Anthony	+1 202 662 5105	santhony@cov.com
Bruce Baird	+1 202 662 5122	bbaird@cov.com
Lanny Breuer	+1 202 662 5674	lbreuer@cov.com
Jason Criss	+1 212 841 1076	jcriss@cov.com
Christopher Denig	+1 202 662 5325	cdenig@cov.com
Arlo Devlin-Brown	+1 212 841 1046	adevlin-brown@cov.com
Steven Fagell (Co-Chair)	+1 202 662 5293	sfagell@cov.com
James Garland	+1 202 662 5337	jgarland@cov.com
Ben Haley	+1 202 662 5194	bhaley@cov.com
Barbara Hoffman	+1 212 841 1143	bhoffman@cov.com
Eric Holder	+1 202 662 6000	
Mitch Kamin	+1 424 332 4800	mkamin@cov.com
Robert Kelner	+1 202 662 5503	rkelner@cov.com
Nancy Kestenbaum	+1 212 841 1125	nkestenbaum@cov.com
Adem Koyuncu	+32 (0)254 95240	akoyuncu@cov.com
Aaron Lewis	+1 424 332 4754	alewis@cov.com
David Lorello	+44 (0)20 7067 2012	dlorello@cov.com
Mona Patel	+1 202 662 5797	mpatel@cov.com
Mythili Raman	+1 202 662 5929	mraman@cov.com
Don Ridings (Co-Chair)	+1 202 662 5357	dridings@cov.com
Dan Shallman	+1 424 332 4752	dshallman@cov.com
Doug Sprague	+1 415 591 7097	dsprague@cov.com
Anita Stork	+1 415 591 7050	astork@cov.com
Daniel Suleiman	+1 202 662 5811	dsuleiman@cov.com
Alan Vinegrad	+1 212 841 1022	avinegrad@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to [unsubscribe@cov.com](mailto:unsubscribe@cov.com) if you do not wish to receive future emails or electronic alerts.