Baker McKenzie.

Dispute Resolution
Beijing/Hong Kong/Shanghai

Client Alert

February 2020

Hong Kong Court confirms the SFC's investigation powers over digital devices in search operations

For further information, please contact:

Cynthia Tang
Partner
+852 2846 1708
cynthia.tang@bakermckenzie.com

Bryan Ng
Partner
+852 2846 2923
bryan.ng@bakermckenzie.com

Cheryl Tang
Associate
+852 2846 1810
cheryl.tang@bakermckenzie.com

In five recent judicial review applications brought against the Securities and Futures Commission (SFC) and the Magistrate (HCAL 2132, 2133, 2134, 2136 and 2137/2018), the Court of First Instance dismissed challenges to the SFC's decisions to seize and retain digital devices during its search operations. The Court has confirmed the wide scope of documents that can be seized by the SFC and the SFC's power to require production of passwords to email accounts or digital devices.

Under the Securities and Futures Ordinance (SFO), the SFC is empowered, among other things, to require production of relevant information, compel a person to attend an interview for answering questions, and apply to a Magistrate for a search warrant to enter and search premises and seize documents. Such search operations (often referred to as "dawn raids") can include a company's office premises or an individual's private residence.

Our alert discusses the implications of the Court's decision and suggests practical steps to better prepare for dawn raids and protect your data.

What it means for you

This decision illustrates the wide range of powers available to the SFC in a search operation and confirms that in addition to seizing and retaining documents in paper form, the SFC also has the power to seize and retain digital devices. Most importantly, the SFC can require the production of login names and passwords to such devices and email accounts.

In our experiences in assisting clients in search operations, it is common for the officers to scroll through emails, instant messages, documents and pictures contained in mobile phones and computers during their search operations. They also perform keyword searches to ascertain whether the devices contain materials relevant to the investigation before deciding whether to seize the digital devices concerned. Concerns over privacy are usually raised. The Court has reinforced the legal principle that the right to privacy is not absolute and considers that the aforesaid practices are in fact reasonable and practical safeguards to protect the privacy of the individuals concerned.

Challenges to SFC's investigation powers dismissed

In 2017, the SFC commenced investigations into possible breaches of the SFO in relation to the listing of a company listed in Hong Kong and the bond placements by two other listed companies. In July 2018, the SFC applied to the magistrate for search warrants authorizing the SFC to "search for, seize and remove" records and documents at the residences of various individuals and the offices of a relevant company. On 5 July 2018, the SFC conducted a search operation to execute the search warrants issued by the magistrate.

In the judicial review applications, the applicants challenged the constitutionality and legality of the SFC's decisions to seize and retain their computers and mobile phones, and requests for the login names and passwords to the email accounts and digital devices. They challenged the decisions on the grounds that they were *ultra vires* the SFO and the validity of the search warrants for want of specificity.

The Court dismissed the judicial review applications and confirmed the SFC's investigation powers in a search operation. This decision is significant in a number of aspects:

- The Court confirmed that the SFC has power to seize digital devices. The terms “document” or “record” in the SFO should be given a very wide meaning and are not confined to records or documents in paper form. This is particularly so given data are nowadays being created, transmitted and stored in digital devices in almost all aspects of daily and commercial activities.

- The Court ruled that the SFC has the power to require the applicants to provide means of access to email accounts and digital devices which contain, or are likely to contain, information relevant to its investigations. This is despite the fact that the email accounts and digital devices might likely contain other personal materials which are not relevant to the SFC’s investigations.

- It is also useful to note the Court's view that there is no requirement under the SFO that a search warrant must include a protocol on how the contents of the digital devices should be examined by the SFC's officers for the purpose of protecting the individuals' privacy.

Actions to take

This decision serves as a useful reminder for listed companies and licensed corporations to review their internal policies regarding the use and storage of electronic data.

We recommend that companies manage any risks or exposure arising from unannounced dawn raids and take the following steps:

- Seek legal assistance from experienced teams promptly in the event of a dawn raid.

- Devise a dawn raid protocol and conduct trainings for staff.

- Review internal policies on employees' use and storage of electronic data, including data stored on company-issued and personal devices.

- Restrict and monitor employees' use of instant messaging applications (such as WeChat and WhatsApp) for work purposes.

- Review electronic data backup system to guard against disruptions to operations even if electronic devices are seized.

- Segregate communications and documents which are protected by legal professional privilege and preserve legal privilege.

www.bakermckenzie.com

Suite 3401, China World Tower 2
1 Jianguomenwai Dajie
Beijing 100004, China
Tel: +86 10 6535 3800
Fax: +86 10 6505 2309

14th Floor, One Taikoo Place
979 King’s Road
Quarry Bay
Hong Kong SAR
Tel: +852 2846 1888
Fax: +852 2845 0476

Unit 1601, Jin Mao Tower
88 Century Avenue, Pudong
Shanghai 200121, China
Tel: +86 21 6105 8558
Fax: +86 21 5047 0020