Hong Kong High Court Dismisses Judicial Review Challenging the SFC's Investigative Powers

March 11, 2020

The Hong Kong High Court has recently dismissed applications for judicial review of search warrants obtained by the Securities and Futures Commission (the "SFC") and the SFC's seizure and retention of digital devices pursuant to the search warrants.

JUDGMENT IN CHEUNG KA HO CYRIL & ORS V. SFC [2020] HKCFI 270

In support of two ongoing investigations into possible breaches of the Securities and Futures Ordinance (the "SFO"), the SFC obtained from the Magistrates' Court search warrants to "*search for, seize and remove records and documents*" at five premises. In July 2018, the SFC conducted search operations based on the search warrants and seized various digital devices. Subsequently, the SFC issued notices under s183(1) of the SFO requiring that login names and passwords to email accounts and digital devices be provided.

The applicants applied for judicial review to challenge the lawfulness of the search warrants, the SFC's decisions to seize and retain their digital devices and the request for login names and passwords. The Court dismissed the applications upon consideration of the merits.

The applicants' challenge against the lawfulness and validity of the search warrants due to lack of specificity

The Court considered that there was "*no overriding or overarching requirement for specificity*" in a search warrant outside the relevant statutory provisions and it was satisfied that the search warrants in this case stated matters that were required under s191(1) of the SFC, *i.e.*:

- the magistrate's satisfaction that there is or is likely to be on certain specified premises any record or document that may be required to be produced under Part VIII of the SFO;

- the persons authorised to execute the warrant and the premises authorised to be entered and searched;

- the authorisation given to search for, seize and remove any record or document which the authorised persons had reasonable cause to believe may be required to be produced under Part VIII of the SFO; and

- the validity period of the search warrant.

Even if, contrary to the Court's view, there was a requirement for a search warrant to specify the offence or misconduct in respect of which it was applied for, the Court was satisfied that the search warrants in question had sufficiently specified the grounds on which records and documents might be required to be produced. It would be impracticable to be more specific about the offences or misconduct at an investigative stage and those details might in any event be subject to secrecy obligations.

The Court also considered that s191 of the SFO did not require the search warrants to set out a protocol on how the examination of digital devices should be carried out by the SFC's officers.

The applicants' challenge against the SFC's decision to seize and retain digital devices

Upon examination of the definitions of "*document*" and "*record*" under the SFO, the Court considered that those words should not be narrowly construed as to "*cripple*" the SFC's investigative powers and instead the wide definitions of those words clearly and amply empowered the SFC to seize the digital devices. This is particularly so when taking into account how most information and data are now created, transmitted, kept and stored.

The Court also considered each of the elements in the four-step proportionality test in assessing the lawfulness of the restriction to the applicants' right to privacy (legitimate aim, rational connection, no more than reasonably necessary, fair balance) was satisfied. In particular, during the search operation the SFC's officers returned to the applicants the devices that did not appear to contain relevant materials and the SFC applied keyword searches and reviewed the contents of the devices together with the applicants in order to minimize the chance of personal or irrelevant information being viewed.

The Court further noted that the digital devices were sanctioned by warrants issued by judicial officers, who could be expected to "*carefully scrutinize the sufficiency of the bases of the applications for the warrants as well as the scope or width of the warrants prior to their issue with an independent mind balancing all relevant conflicting interests*".

Since the seizure of the digital devices was considered to be lawful, the SFC was also entitled to retain the records for at least six months under s193(3) of the SFO.

The applicants' challenge against the SFC's request to provide login names and passwords

For the same reasons concerning the validity of the search warrants, the Court considered that the SFC was empowered, under s183(1) of the SFO, to require the applicants to provide means of access to email accounts and digital devices which contained or were likely to contain relevant information.

The Court noted that the SFC's approach to use keyword searches was safeguards to protect the privacy of the applicants as the email accounts and digital devices would likely also contain other personal or private materials irrelevant to the investigations.

SIGNIFICANCE

In view of the Court's confirmation of the scope of the SFC's investigative powers, it is expected that more investigations conducted by the SFC will involve search warrants for "*records and documents*" and requests to access the data contained in the seized devices. The decision also highlights the importance of the regulator to providing sufficient safeguards to protect the individuals' privacy in the investigations.

The decision is a reminder that regulated firms and listed companies should establish a response plan in the event that the SFC executes a search warrant at the premises. Such a response plan would involve:

Advance planning

- Set up a dedicated response team–the team should include a member of the senior management team, a secretarial/administrative office, an IT officer and a legal advisor;
- Provide sufficient training to employees and ensure they know whom to call when a search is requested;
- Ensure that the IT systems back up data of hard disk drives, email servers and files; and
- Maintain proper record retention policy–including practices of marking potentially confidential and/or privileged documents.

Initial response and good practices during a search operation

- Seek legal advice immediately and request legal advisors to attend at the premises as soon as possible;
- Prepare one or more meeting rooms for the investigators;
- Verify the identities and authority of the investigators and the location specified on the warrant;
- Take photocopies of the warrant and identifications of the attending investigators;
- Arrange for each investigator to be accompanied by either a member of staff or a legal advisor during the search operation;
- Keep a record of the search including the areas visited, the people spoken to, what was said and what records and documents were requested, inspected, copied and/or seized;
- Ensure that no privileged documents are handed over until they have been reviewed by legal advisors;
- Photocopy all seized documents and compare them against the inventory list prepared by the investigators;
- Answer any questions raised by investigators during the search operation in writing after taking legal advice. If that is not possible, answers provided should not be misleading; and
- Ensure that employees are aware of their secrecy obligations.

* * *

Please do not hesitate to contact us with any questions.

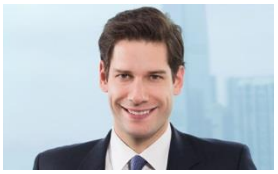
HONG KONG


Gareth Hughes
Partner
ghughes@debevoise.com


Mark Johnson
Partner
mdjohnson@debevoise.com


Emily Lam
International Counsel
elam@debevoise.com


Tiffany Chan
Associate
tchan@debevoise.com


Ralph Sellar
Associate
rsellar@debevoise.com


Elly Tso
Associate
etso@debevoise.com