KIRKLAND & ELLIS

Kirkland Alert

Hong Kong Financial Markets Regulator's Power to Seize Electronic Devices Provides Increased Scope for Financial Crimes Enforcement

29 April 2020

On February 14, 2020, the Hong Kong High Court handed down a judgment (*Cheung Ka Ho Cyril and others v Securities and Futures Commission* (HCAL 2132-4, 2136-7/2018, unreported) dismissing challenges to the powers of the Securities and Futures Commission ("SFC") to seize and retain digital devices as part of its search operations. Significantly, the court confirmed the wide scope of documents that may be seized by the SFC under the Securities and Futures Ordinance (Cap. 571) (the "SFO"), and the SFC's power to require production of digital devices and to compel production of the passwords to such digital devices and their associated email accounts.

Under the SFO, the SFC is empowered to require production of information relevant to an investigation (a "Section 183(1) Notice"), to compel a person to attend an interview, and to apply for a search warrant to enter and search premises and to seize documents found therein. The premises at which such warrants may be executed by the SFC include a company's offices and the location of its email and file servers, or an individual's private residence.

In light of the recent obligation of licensed corporations and registered institutions to disclose details of internal investigations to the SFC (see below), and the Memorandum of Understanding (the "MOU") for greater cooperation recently entered between the SFC and the Independent Commission Against Corruption ("ICAC"), it is increasingly important that licensed entities and registered institutions are fully aware of the investigative powers of the relevant authorities, promptly review their internal policies and actively manage any risks or exposure arising from unannounced dawn raids.

Background

The *Cheung Ka Ho* case arose from two separate ongoing investigations conducted by the SFC involving the execution of search warrants issued by magistrates on multiple premises. On the basis of these warrants, the SFC seized a number of digital devices including mobile phones, tablets and personal computers. Where no password was required to access such devices, the SFC forensically analysed the devices using keyword searches to check for relevant information. Where the Applicants voluntarily unlocked the devices on-site, the SFC used keyword searches or scrolled through the device contents to identify relevant materials. As a result of these searches, the SFC identified materials contained in emails, contact lists and instant messaging applications on the seized devices that were relevant, or likely to be relevant, to its investigations. Where the Applicants either declined to provide printouts of the relevant materials or the login names and passwords to certain email accounts or digital devices, the SFC seized and impounded the relevant devices and proceeded to issue Section 183(1) Notices to the Applicants, requesting a wide range of information including the contested login names and passwords.

The Applicants applied for judicial review of a number of the issued search warrants, as well as related decisions made by the SFC in the course of its execution of these search warrants. The Applicants' grounds were as follows: (a) whether the SFC's decisions to seize and retain certain digital devices were outside the scope of the SFO or the search warrants, which would render them unlawful and/or unconstitutional; (b) whether the decisions of the SFC to issue Section 183(1) Notices requiring the Applicants to provide the SFC with the passwords to their email accounts or devices were unconstitutional; and (c) whether the search warrants were invalid for want of specificity.

The court dismissed these applications and confirmed the SFC's wide-ranging investigative powers in a search operation. This decision is significant due to the following findings:

- The court noted that the terms "document" and "record" are defined broadly under the SFO and are not confined to records or documents in the traditional sense, given that data is created, stored and transmitted in digital devices in almost all aspects of daily and commercial activities.
- The SFC has the power to require individuals and companies to provide a means of access to email accounts and digital devices that contain, or are likely to contain, information relevant to its investigations. Although the Applicants argued that the

digital devices likely contained other personal data that were irrelevant to the SFC's investigations, it was held that the SFC had no reasonable or practicable alternative but to seize the digital devices. The interference with the Applicants' privacy was held to be no more than reasonably necessary under the circumstances.

- The court held that there is no requirement under the SFO for a search warrant to particularise the documents or records to be seized, nor did the Ordinance require the SFC to institute any protocol on how the contents of the digital devices should be examined by its officers to protect the individuals' privacy.

Key Takeaways

It is anticipated that listed companies in Hong Kong, licensed persons and other registered institutions regulated by the SFC will increasingly be subject to greater scrutiny by regulators in respect of financial crimes and corruption in the securities and futures markets. For instance, as part of the 2020–2021 Budget, the government recently announced the creation of a dedicated police bureau specialising in financial crimes investigations, which would double the number of its AML/CTF investigators.

The *Cheung Ka Ho* decision also comes on the back of significant steps undertaken by the SFC to enhance the licensing and reporting regime and to coordinate investigations with other regulators for financial crimes. In April 2019, the SFC implemented a new obligation for licensed corporations and registered institutions to disclose if their departing licensed representatives, responsible officers and executive officers had been the subject of any internal investigation (relating to **both** regulated and unregulated activities) in the six months prior to their departure, and to report the details of such investigations to the SFC.[1] In addition, in August 2019, the SFC and the ICAC entered into a MOU to enhance their collaboration and formalise their cooperation in investigating financial crime. The MOU allows both regulators to exchange information to assist the other in discharging its functions, to refer matters to the other agency, to conduct joint investigations and to provide other mutual investigative assistance.

Although details of internal investigations disclosed to the SFC under the above-mentioned disclosure obligation would not be disclosed to third parties, the SFC has the power to refer such details to its Enforcement Division for further review. An internal investigation, once disclosed, may therefore trigger a Section 183(1) Notice and a compulsory interview under Section 183 of the SFO. During an interview conducted under this section, the interviewee would not have the right to remain silent on the basis of self-incrimination, and any failure to answer questions or to answer

fully would constitute a criminal offence (section 184 of the SFO). While any evidence obtained during such an interview could not be used directly against the interviewee in a subsequent criminal proceeding, it could be used by the SFC (or the ICAC) in criminal proceedings against others, including co-conspirators of the interviewee (section 378(3)(i)). The SFC and the ICAC would also be able to utilise the compulsorily obtained information in a derivative manner: Any other materials that the interview led the investigators to identify, or helped them to discover, could be used in subsequent criminal proceedings against the interviewee **or** others.

This significant decision bolsters the SFC's investigative arsenal by confirming its power to demand passwords to digital devices or email accounts accessible from such devices wherever the SFC has reasonable cause to believe that the devices or emails in those accounts contain, or are likely to contain, information relevant to an investigation. SFC officers will, as a matter of practice, scroll through emails, instant messages (such as WhatsApp and WeChat accounts), documents and pictures contained in mobile phones, tablets and personal computers during their search operations, and will perform keyword searches to determine whether the devices contain any materials relevant to the investigation before deciding whether to seize the devices. Although an individual has a right to privacy with regard to personal information held on such devices that is irrelevant to the investigation, the court held that under the circumstances, the risk of infringing this right was outweighed by the need to conduct an effective investigation.

It is important for companies to consider the practical implications of the *Cheung Ka Ho* case, and to assess the extent to which employees' portable digital devices are connected to the company's online systems and databases, given that it may be possible for the SFC to demand that individuals log into proprietary systems on their devices pursuant to a Section 183(1) Notice. As regulatory and compliance risks become more interconnected under the current Hong Kong enforcement climate, it is critical that companies consult regulatory counsel promptly to review their risk management policies and procedures for responding to internal investigations and dawn raids, and to actively manage the potential follow-on legal exposure arising from unannounced dawn raids.

---

1. FAQ on Disclosure of investigations commenced by licensed corporations in the notifications of cessation of accreditation: https://www.sfc.hk/web/EN/faqs/intermediaries/licensing/disclosure-of-investigations-commenced-by-licensed-corporations.html.↩

Authors

Cori A. Lable

Partner / Hong Kong

Richard Sharpe

Partner / Hong Kong

Gerald Lam

Associate / Hong Kong

Related Services

Practices

- Litigation
- Government, Regulatory & Internal Investigations
- International Risk & Investigations
- Data Security & Privacy