March 25 Legal and Regulatory Update

Top stories

SFC's major enforcement efforts

SFC's publication *(Enforcement Reporter)* highlighted its major enforcement efforts to combat corporate misconduct.

Firstly, it introduced a **new Market scanning detection model to identify governance red flags for early intervention. The goal is to prevent** rather than to discipline. **AI-empowered analytics** are employed to assess financial disclosures, market trends, and governance indicators to identify companies with elevated risk profiles.

SFC will **proactively engage with company boards and audit committees** to highlight key risk areas and governance concerns.

Secondly, it recaps its **2023 Joint statement with AFRC** which highlighted an observed increase in suspected misconduct by listed issuers using **dubious loans, advances, and prepayments** to divert funds. The statement emphasised the need for proper conduct and governance among management, audit committees, and auditors.

Enforcement cases demonstrating SFC's resolve to **obtain compensation for minority shareholders** *(including **disqualification** and **compensation orders**)* were highlighted. **Key insights** on lessons learnt were set out.

In a compensation and disqualification orders case *(P.11)* , a **CFO** was found to have allowed funds to be misappropriated by the then chairman. SFC highlighted that those who commit or assist incorporate misconduct can be and will be held accountable, even if they may not have personally received the illegal proceeds. i.e. despite the **absence of personal financial benefits.**

The Mar 2025 case on 3DG Holdings (International) Limited is set out in the section below.

Also in this issue

Regulators

(i) SFC seeks disqualification and compensation orders against the entire former board of 3DG Holdings (International) Limited. (Press release)

SFC has commenced legal proceedings in the Court of First Instance *(s. 214, Securities and Futures Ordinance)*, seeking **disqualification and compensation orders against the entire former board**, **including independent directors (INEDs)**.

Background: the case involved alleged failure in preventing **misappropriation of corporate funds**. In 2017, the company acquired a 100% equity interest in a company with a money lender's licence. It granted 12 loans *(total: $74.4 million)* through its new money lending business, but all of the loans were in default when they came due.

As part of the legal action, the SFC is seeking **compensation orders** against the directors to pay, whether individually or jointly and severally, the company the sum of $74.4 million, being the cash paid out for the 12 loans. Specifically, the SFC alleges that the acquisition and the loans formed part of a scheme to misappropriate the company's cash.

What you should watch out for

In its Enforcement Reporter *(P.6)* , SFC highlighted that its actions "underscore that **INEDs are not merely symbolic appointments** but are expected to exercise independent judgment and proactive oversight. Independent directors play a crucial role in ensuring proper corporate governance, and their **failure to act with adequate skill, care, and diligence can have severe consequences**."

(ii) SFC has obtained a disqualification order on the former financial controller (FC) of Anxin-China Holdings Limited for 3 years. (Press release)

Background: The company grossly overstated its cash position between 2011-5, in particular, cash position in audited consolidated financial statements for the 2 years ending 31 Dec 2012 and 13 *(overstated by $1.26 billion and $1.73 billion)*. To cover up, it provided false bank records to its auditors.

FC admitted liability as (A) financial controller, (B) a member of the special team formed to investigate into discrepancies identified by the auditors in re: banking records and management accounts.

In the press release, **SFC** stated that: "**The role of financial controllers** in listed companies is pivotal to ensuring the integrity of financial reporting. **Professional scepticism** is not just a best practice; it is an essential duty. Financial controllers must approach their responsibilities with a critical mindset, actively questioning and verifying financial information to protect stakeholders."

What you should watch out for

Specific failures

FINANCIAL CONTROLLER

- Required to have a detailed understanding of financial condition, including cash reserves
- Failed to take reasonable steps which would have enabled realisation of "over-stated cash position"

INVESTIGATION TEAM MEMBER

- Failed to take steps to verify the team's findings
- Did not take steps to voice out
    - Concerns re: cash flow and the bank records provided to the independent forensic investigator
    - Suspicions re: integrity of senior management

(iii) HKEX **re-grouped Enforcement Bulletins** *(published since 2017)* **by topics** for easy reference. E.g. Directors and senior management.

Legislation

(iii) Privacy Commissioner for Personal Data (PCPD) published (A) Checklist on Guidelines for the use of Generative AI (Gen AI) by employees and (B) Investigation findings on the data breach Incident of ImagineX Management Company Limited (Press release)

(A) Guidelines

These aim to **assist organisations in developing internal policies or guidelines** on the use of Gen AI by employees at work while complying with the requirements of the Personal Data (Privacy) Ordinance (PDPO). (Guidelines)

The Guidelines recommend that organisations **cover the following aspects when developing their internal policies or guidelines**. **Key elements** include:

- **Scope**
  - **Permitted tools** *(e.g. publicly available and/or internally developed Gen AI tools)*
  - **Permissible use** *(e.g. drafting)*
  - **Policy applicability** *(e.g. for the whole organisation, or specific department)*
- **Protection of personal data privacy**
  - **Permissible types/amounts of input information**
    - e.g. **not permitted** *(e.g. personal, confidential, proprietary of copyrighted data)*
  - **Permissible use of output information**
  - **Permissible storage of output information**
  - **Other relevant internal policies** *(e.g. on information security)*
- **Lawful and ethical use and prevention of bias**
  - Include emphasising the need for employees to verify the information provided by AI *(e.g. fact-checking)*
- **Data security**
  - **Permitted devices** to access Gen AI tools *(e.g. office computers)*
  - **Permitted users**
  - **Robust user credentials**
  - Maintain **stringent security settings** in Gen AI tools
  - Response to **AI incident and data breach incidents**
- **Violations of policies or guidelines**
  - Specify the possible consequences
  - Tips on **AI governance** *(refer to PCPD's AI Model framework; see our June 24 update)*

(B) ImagineX breach incident

ImagineX is a brand management and distribution company for international fashion/beauty businesses and manages membership programmes. It submitted a data breach notification to PCPD in May 24, that it received a ransom note from a threat actor.

The threat actor compromised a temporary user account created for ImagineX's vendor for urgent remote support. It gained access to ImagineX's network, exploited a vulnerability in an application server that was running an end-of-support operating system to further penetrate servers containing personal data.

2 loyalty programmes were affected *(ICARD, Brook Brothers),* involving **127,268** individuals, their email addresses, telephone numbers, birth months, genders, nationalities of the members.

What you should watch out for

Deficiencies identified by PCPD

- **Failure to delete temporary account timely**
- **Use of end-of-support operating system**
- **Ineffective detective measures for information systems**
- **Insufficient security risk reviews and audits**

Published by Practising Governance Limited

April 2025