



24 November 2020

NOTICE

RE: Financial Sanctions Notice

The Cayman Islands Monetary Authority ("CIMA") hereby notifies you that it has received a new Notice from the Office of Financial Sanctions Implementation, HM Treasury ("OFSI"), which is attached as an Annex to this Notice.

1. What you must do:

- A. In the case of an addition or amendment of a person to the [Consolidated List](#) and asset freeze:
 - i. Check whether you maintain any accounts or hold any funds or economic resources for the persons set out in the OFSI Notice;
 - ii. Freeze any such accounts and other funds or economic resources.
 - iii. Refrain from dealing with the funds or assets or making them available (directly or indirectly) to such persons unless licensed by the Governor.
 - iv. Report any findings to the Financial Reporting Authority ("FRA") at financialsanctions@gov.ky together with any additional information that would facilitate compliance with the relevant legislative requirements.
 - v. Provide any information concerning the frozen assets of designated persons to the FRA at financialsanctions@gov.ky and submitting a compliance reporting form. Information reported to FRA may be passed to other regulatory authorities or law enforcement.

- B. In the case of the removal of a person from the [Consolidated List](#) and unfreezing of assets
 - i. Check whether you have frozen assets of any person or entity removed from the Consolidated List and verify that the person is no longer subject to an asset freeze.
 - ii. Remove the person from your institution's list of persons or entities subject to financial sanction.
 - iii. Un-freeze the assets of the person and where necessary re-activate all relevant accounts.

- iv. Send advice to the person that the assets are no longer subject to an asset freeze.
 - v. Advise the FRA at financialsanctions@gov.ky of the actions taken.
2. Failure to comply with financial sanctions legislation or to seek to circumvent its provisions is a criminal offence.

Further Information.

For general information on financial sanctions please see FRAs Industry Guidance on targeted financial sanctions.

[http://fra.gov.ky/app/webroot/files/2020-02-21%20FRA%20Financial%20Sanctions%20Guidance%20\(Final\).pdf](http://fra.gov.ky/app/webroot/files/2020-02-21%20FRA%20Financial%20Sanctions%20Guidance%20(Final).pdf).

Enquiries regarding this sanctions notice should be addressed to
The Sanctions Coordinator
Financial Reporting Authority
P.O. Box 1054
Grand Cayman KY1-1102
Cayman Islands
FinancialSanctions@gov.ky

REGIME: Cyber-Attacks

INDIVIDUAL

1. **Names (Last):** Gao **(1):** Qiang **(2):** n/a **(3):** n/a **(4):** n/a **(5):** n/a

Title: n/a

Position: n/a

A.K.A: n/a

Date of Birth: 04/10/1983

Place of Birth: Shandong Province

Nationality: Chinese

Passport Details: n/a

Address: Room 1102 Guanfu Mansion 46 Xinkai Road Hedong District Tianjin China

Other Information Gender: male. Gao Qiang is involved in “Operation Cloud Hopper”, a series of cyber-attacks. “Operation Cloud Hopper” targeted information systems of multinational companies in six continents, including companies located in the European Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (a.k.a. “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Gao Qiang can be linked to APT10, including through his association with APT10 command and control infrastructure. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating “Operation Cloud Hopper”, employed Gao Qiang. He has links with Zhang Shilong, who is also designated in connection with “Operation Cloud Hopper”. Gao Qiang is therefore associated with both Huaying Haitai and Zhang Shilong.

Listed On: 31/07/2020

Last Updated: 24/11/2020

Group ID: 13903

Names (Last): **Zhang (1): Shilong (2): n/a (3): n/a (4): n/a (5): n/a**

Title: **n/a**

Position: **n/a**

A.K.A: **n/a**

Date of Birth: **10/09/1981**

Place of Birth: **n/a**

Nationality: **Chinese**

Passport Details: **n/a**

Address: **Hedong Yuyang Road No 121 Tianjin China**

Other Information **Gender: male. Zhang Shilong is involved in “Operation Cloud Hopper”, a series of cyber-attacks. “Operation Cloud Hopper” has targeted information systems of multinational companies in six continents, including companies located in the European Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (a.k.a. “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Zhang Shilong can be linked to APT10, including through the malware he developed and tested in connection with the cyber-attacks carried out by APT10. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating “Operation Cloud Hopper”, employed Zhang Shilong. He has links with Gao Qiang, who is also designated in connection with “Operation Cloud Hopper”. Zhang Shilong is therefore associated with both Huaying Haitai and Gao Qiang.**

Listed On: **31/07/2020**

Last Updated: **24/11/2020**

Group ID: **13904**