



31 July 2020

NOTICE

RE: Financial Sanctions

1. 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.
2. **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.
3. Failure to comply with financial sanctions legislation or to seek to circumvent its provisions is a criminal offence.

Further Information.

4. 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).
5. 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: n/a
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: **31/07/2020**
Group ID: 13903

2. **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: n/a
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: 31/07/2020
Group ID: 13904
3. **Names (Last):** Minin **(1):** Alexey **(2):** Valeryevich **(3):** n/a **(4):** n/a **(5):** n/a
Title: n/a
Position: n/a
A.K.A: n/a
Date of Birth: 27/05/1972
Place of Birth: Perm Oblast
Nationality: Russian
Passport Details: 120017582. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022
Address: Moscow Russian Federation
Other Information Gender: male. Alexey Minin took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Alexey Minin was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work.
Listed On: 31/07/2020
Last Updated: 31/07/2020
Group ID: 13905
4. **Names (Last):** Morenets **(1):** Aleksei **(2):** Sergeyvich **(3):** n/a **(4):** n/a **(5):** n/a
Title: n/a
Position: n/a
A.K.A: n/a

Date of Birth: 31/07/1977

Place of Birth: Murmanskaya Oblast

Nationality: Russian

Passport Details: 100135556. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022

Address: Moscow Russian Federation

Other Information Gender: male. Aleksei Morenets took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Aleksei Morenets was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work.

Listed On: 31/07/2020

Last Updated: 31/07/2020

Group ID: 13906

5. **Names (Last):** Serebriakov **(1):** Evgenii **(2):** Mikhaylovich **(3):** n/a **(4):** n/a **(5):** n/a

Title: n/a

Position: n/a

A.K.A: n/a

Date of Birth: 26/07/1981

Place of Birth: Kursk

Nationality: Russian

Passport Details: 100135555. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022

Address: Moscow Russian Federation

Other Information Gender: male. Evgenii Serebriakov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Evgenii Serebriakov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work.

Listed On: 31/07/2020

Last Updated: 31/07/2020

Group ID: 13907

6. **Names (Last):** Sotnikov **(1):** Oleg **(2):** Mikhaylovich **(3):** n/a **(4):** n/a **(5):** n/a

Title: n/a

Position: n/a

A.K.A: n/a

Date of Birth: 24/08/1972

Place of Birth: Ulyanovsk

Nationality: Russian

Passport Details: 120018866. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022

Address: Moscow Russian Federation

Other Information Gender: male. Oleg Sotnikov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW), in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Oleg Sotnikov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work.

Listed On: 31/07/2020

Last Updated: 31/07/2020

Group ID: 13908

ENTITY

1. **Names (Last):** Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai) **(1):** n/a **(2):** n/a **(3):** n/a **(4):** n/a **(5):** n/a

A.K.A: Haitai Technology Development Co. Ltd

Other Information Huaying Haitai provided financial, technical or material support for and facilitated "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". Huaying Haitai can be linked to APT10. Moreover, Huaying Haitai employed Gao Qiang and Zhang Shilong, who are both designated in connection with "Operation Cloud Hopper". Huaying Haitai is therefore associated with Gao Qiang and Zhang Shilong.

Listed On: 31/07/2020

Last Updated: 31/07/2020

Group ID: 13909

2. **Names (Last):** Chosun Expo **(1):** n/a **(2):** n/a **(3):** n/a **(4):** n/a **(5):** n/a

A.K.A: (1) Chosen Expo, (2) Korea Export Joint Venture

Other Information Chosun Expo provided financial, technical or material support for and facilitated a series of cyberattacks, including the cyber-attacks publicly known as "WannaCry" and cyber-attacks against the Polish Financial Supervision Authority and Sony Pictures Entertainment, as well as cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank. "WannaCry" disrupted information systems around the world by targeting information systems with ransomware and blocking access to data. It affected information systems of companies in the European Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States. The actor publicly known as "APT38" ("Advanced Persistent Threat 38") or the "Lazarus Group" carried out "WannaCry". Chosun Expo can be linked to APT38 / the Lazarus Group, including through the accounts used for the cyber-attacks.

Listed On: 31/07/2020

Last Updated: 31/07/2020

Group ID: 13910

3. **Names (Last):** Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) **(1):** n/a **(2):** n/a **(3):** n/a **(4):** n/a **(5):** n/a

A.K.A: n/a

Other Information The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known by its field post number 74455, is responsible for cyber-attacks, including the cyber-attacks publicly known as "NotPetya" or "EternalPetya" in June 2017 and the cyber-attacks directed at an Ukrainian power grid in the winter of 2015 and 2016. "NotPetya" or "EternalPetya" rendered data inaccessible in a number of companies in the European Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting amongst others in significant economic loss. The cyber-attack on a Ukrainian power grid resulted in parts of it being switched off during winter. The actor publicly known as "Sandworm" (a.k.a. "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" and "Telebots"), which is also behind the attack on the Ukrainian power grid, carried out "NotPetya" or "EternalPetya". The Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation has an active role in the cyber-activities undertaken by Sandworm and can be linked to Sandworm.

Listed On: 31/07/2020

Last Updated: 31/07/2020

Group ID: 13911

REGIME: The ISIL (Da'esh) and Al-Qaida organisations

INDIVIDUAL

1. **Names (Last):** D'Ancona **(1):** Bryan **(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: 26/01/1997

Place of Birth: Nice

Nationality: French

Passport Details: n/a

Address: n/a

Other Information EU listing only.

Listed On: 31/07/2020

Last Updated: 31/07/2020

Group ID: 13902