23 October 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%20Santions%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: Chemical Weapons

INDIVIDUAL

1. **Names (Last):** Kostyukov **(1):** Igor **(2):** Olegovich **(3):** n/a **(4):** n/a **(5):** n/a
Title: n/a
Position: Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU/GU)
A.K.A: n/a
Date of Birth: 21/02/1961
Place of Birth: n/a
Nationality: Russian
Passport Details: n/a
Address: n/a
Other Information Gender: male. Igor Olegovich Kostyukov, given his senior leadership role as First Deputy Head of the GRU (a.k.a. GU) at that time, is responsible for the possession, transport and use in Salisbury during the weekend of 4 March 2018 of the toxic nerve agent 'Novichok' by officers from the GRU. One of the units under his command is the 85th Main Centre for Special Services (GTsSS), also known as 'military unit 26165' (industry nicknames: 'AP28', 'Fancy Bear', 'Sofacy Group', 'Pawn Storm' and 'Strontium'). In this capacity Igor Kostyukov is responsible for cyber-attacks carried out by the GTsSS. In particular, the cyber-attack against the German federal parliament which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. Listed under both the Chemical Weapons and Cyber-Attacks regimes.
Listed On: 21/01/2019

Last Updated: 23/10/2020
Group ID: 13748

REGIME: Cyber-Attacks

INDIVIDUAL

1. **Names (Last):** Badin **(1):** Dmitry **(2):** Sergeyevich **(3):** n/a **(4):** n/a **(5):** n/a
Title: n/a
Position: n/a
A.K.A: n/a
Date of Birth: 15/11/1990
Place of Birth: Kursk
Nationality: Russian
Passport Details: n/a
Address: n/a
Other Information Gender: male. As a military intelligence officer of the 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Dmitry Badin was part of a team of Russian military intelligence officers which conducted a cyber-attack against the German federal parliament in April and May 2015.
Listed On: 23/10/2020
Last Updated: 23/10/2020
Group ID: 13983

2. **Names (Last):** Kostyukov **(1):** Igor **(2):** Olegovich **(3):** n/a **(4):** n/a **(5):** n/a
Title: n/a
Position: Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU/GU)
A.K.A: n/a
Date of Birth: 21/02/1961
Place of Birth: n/a
Nationality: Russian
Passport Details: n/a
Address: n/a
Other Information Gender: male. Igor Olegovich Kostyukov, given his senior leadership role as First Deputy Head of the GRU (a.k.a. GU) at that time, is responsible for the possession, transport and use in Salisbury during the weekend of 4 March 2018 of the toxic nerve agent 'Novichok' by officers from the GRU. One of the units under his command is the 85th Main Centre for Special Services (GTsSS), also known as 'military unit 26165' (industry nicknames: 'AP28', 'Fancy Bear', 'Sofacy Group', 'Pawn Storm' and 'Strontium'). In this capacity Igor Kostyukov is responsible for cyber-attacks carried out by the GTsSS. In particular, the cyber-attack against the German federal parliament which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. Listed under both the Chemical Weapons and Cyber-Attacks regimes.
Listed On: 23/10/2020

Last Updated: 23/10/2020
Group ID: 13748

ENTITY

1. Names (Last): **85th Main Centre for Special Services (GTsSS) 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 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known as "military unit 26165" (industry nicknames: "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" and "Strontium"), is responsible for cyber-attacks with a significant effect constituting an external threat to the Union or its Member States. In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018.**
   Listed On: **23/10/2020**
   Last Updated: 23/10/2020
   Group ID: **13984**