Office of Financial
Sanctions Implementation
HM Treasury

Financial Sanctions Notice

08/10/2024

Cyber

Introduction

1. The Cyber (Sanctions) (EU Exit) Regulations 2020 (S.I. 2020/597) ("the Regulations") were made under the Sanctions and Anti-Money Laundering Act 2018 ("the Sanctions Act") and provide for the imposition of financial sanctions, namely the freezing of funds and economic resources of persons who are have been involved in cyber activity which undermines, or is intended to undermine, the integrity, prosperity or security of the United Kingdom or a country other than the United Kingdom; directly or indirectly causes, or is intended to cause, economic loss to, or prejudice to the commercial interests of, those affected by the activity; undermines, or is intended to undermine, the independence or effective functioning of an international organisations or a non-government organisation or forum whose mandate or purposes related to the governance of international sport or the Internet; or otherwise affects a significant number of persons in an indiscriminate manner.

2. 4 entries have been corrected on the Consolidated List, bringing the entries in line with the UK Sanctions List.

Notice summary

3. The following entries have been corrected on the Consolidated List and remain subject to an asset freeze:

- Eduard Vitalevich BENDERSKIY (Group ID: 16584)
- Aleksey Evgenyevich SHCHETININ (Group ID: 16586)
- Dmitriy Alekseyevich SLOBODSKOY (Group ID: 16581)
- Maksim Viktorovich YAKUBETS (Group ID: 16583)

What <u>you</u> must do

4. You must:

   i. check whether you maintain any accounts or hold any funds or economic resources for the persons set out in the Annex to this Notice and any entities owned or controlled by them;

   ii. freeze such accounts, and other funds or economic resources;

   iii. refrain from dealing with the funds or economic resources or making them available directly or indirectly to or for the benefit of designated persons unless licensed by the Office of Financial Sanctions Implementation (OFSI) or if an exception applies;

   iv. report any findings to OFSI, together with the information or other matter on which the knowledge or suspicion is based. Where the information relates to funds or economic resources, the nature and quantity should also be reported.

5. Information received by OFSI may be disclosed to third parties in accordance with provisions set out in the Information and Records part of the regulations and in compliance with applicable data protection laws.

6. Failure to comply with UK financial sanctions legislation or to seek to circumvent its provisions may be a criminal offence.

Ransomware and Sanctions

7. Making or facilitating a ransomware payment risks exposing those involved to civil or criminal penalties where such payments are made to designated persons.

8. OFSI, in partnership with other HM Government organisations has published guidance on sanctions and ransomware, which includes information on the impact of ransomware payments, cyber resilience and HM Government's approach to enforcement.

9. Guidance on ransomware and sanctions can be found here: https://www.gov.uk/government/publications/financial-sanctions-faqs.

Further Information

10. Copies of recent notices, UK legislation and relevant guidance can be obtained from the Cyber financial sanctions page on the GOV.UK website: https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases.

11. The Consolidated List can be found here: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets.

12. The UK Sanctions List can be found here: https://www.gov.uk/government/publications/the-uk-sanctions-list.

13. The Compliance Reporting Form can be found here: https://www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do.

14. For more information please see our financial sanctions guidance: https://www.gov.uk/government/publications/financial-sanctions-faqs.

Enquiries

15. Non-media enquiries about the implementation of financial sanctions in the UK should be addressed to:

    Office of Financial Sanctions Implementation
    HM Treasury
    1 Horse Guards Road
    London
    SW1A 2HQ
    ofsi@hmtreasury.gov.uk.

16. Non-media enquiries about the sanctions measures themselves should be addressed to: fcdo.correspondence@fcdo.gov.uk.

17. Media enquiries about how financial sanctions are implemented in the UK should be addressed to the Treasury Press Office on 020 7270 5238.

18. Media enquiries about the sanctions measures themselves should be addressed to the Foreign, Commonwealth & Development Office Press Office on 020 7008 3100.

ANNEX TO NOTICE

FINANCIAL SANCTIONS: CYBER

THE CYBER (SANCTIONS) (EU EXIT) REGULATIONS 2020 (S.I. 2020/597)

CORRECTIONS

Deleted information appears in strikethrough. Additional information appears in italics and is underlined.

Individuals

1. **Benderskiy, Eduard Vitalevich**
   Name (non-latin script): Эдуард Витальевич БЕНДЕРСКИЙ
   DOB: 25/06/1970. ***a.k.a: BENDERSKIY, Eduard, Vitalyevich*** **Other information:** (UK Sanctions List Ref): CYB0057. (UK Statement of Reasons): Eduard Vitalevich BENDERSKIY has been involved in relevant cyber activity, including being responsible for, engaging in and providing support for malicious cyber activity that resulted in the unauthorised access and exfiltration of sensitive data from UK infrastructure and networks. Eduard BENDERSKIY facilitated Evil Corp's connections and involvement with the Russian Intelligence Services and provided both political and physical protection to the group, enabling their malicious cyber operations. Evil Corp's malicious cyber activity involved a concerted effort to compromise UK health, government and public sector institutions, and commercial technology companies, for financial gain, which undermined or was intended to undermine the integrity, prosperity and security of the United Kingdom and its allies. (Gender): Male **Listed on:** 01/10/2024 **UK Sanctions List Date Designated:** 01/10/2024 **Last updated:** ~~01/10/2024~~ *08/10/2024* **Group ID:** 16584.

2. **Shchetinin, Aleksey Evgenyevich**
   Name (non-latin script): Алексей Евгеньевич ЩЕТИНИН
   DOB: 22/08/1987. ***a.k.a: SHCHETININ, Aleksey, Yevgenevich*** **Other information:** (UK Sanctions List Ref): CYB0058. (UK Statement of Reasons): Aleksey Evgenyevich SHCHETININ is a member of Evil Corp, and has been involved in relevant cyber activity, including providing financial services, or making available funds or economic resources, that could contribute to malicious cyber activity that resulted in the unauthorised access and exfiltration of sensitive data from UK infrastructure and networks. He has also provided financial services that could contribute to relevant cyber activity. Aleksey SHCHETININ provided financial services through coordinating the trading of cryptocurrency on behalf of Evil Corp. Evil Corp's malicious cyber activity involved a concerted effort to compromise UK health, government and public sector institutions and commercial technology companies, for financial gain, undermined or was intended to undermine the integrity, prosperity and security of the United Kingdom and its allies. (Gender): Male **Listed on:** 01/10/2024 **UK Sanctions List Date Designated:** 01/10/2024 **Last updated:** ~~01/10/2024~~ *08/10/2024* **Group ID:** 16586.

3. **Slobodskoy, ~~Dmitriy~~ *Dmitry* Alekseyevich**
   Name (non-latin script): Дмитрий Алексеевич СЛОБОДСКОЙ

DOB: 28/07/1988. **Other information:** (UK Sanctions List Ref): CYB0055. (UK Statement of Reasons): Dmitry Alekseyevich SLOBODSKOY is a member of Evil Corp, and has been involved in relevant cyber activity, including being responsible for, engaging in and providing support for malicious cyber activity that resulted in the unauthorised access and exfiltration of sensitive data from UK infrastructure and networks. Dmitry SLOBODSKOY is associated with Aleksandr RYZHENKOV who was a senior member and manager of Evil Corp, and was involved in the development and deployment of ransomware that was used by Evil Corp to carry out its relevant cyber activity. Evil Corp's malicious cyber activity involved a concerted effort to compromise UK health, government and public sector institutions, and commercial technology companies, for financial gain, undermined or was intended to undermine the integrity, prosperity and security of the United Kingdom and its allies. (Gender): Male **Listed on:** 01/10/2024 **UK Sanctions List Date Designated:** 01/10/2024 **Last updated:** ~~01/10/2024~~ *08/10/2024* **Group ID:** 16581.

4. **Yakubets, Maksim Viktorovich**
Name (non-latin script): Максим Викторович ЯАКУБЕЦ
DOB: ~~10/06/1986.~~ *20/05/1987.* **a.k.a:** AQUA **Other information:** (UK Sanctions List Ref): CYB0048. (UK Statement of Reasons): Maksim Viktorovich YAKUBETS is a member of Evil Corp, and has been involved in relevant cyber activity, including being responsible for, engaging in and providing support for malicious cyber activity that resulted in the unauthorised access and exfiltration of sensitive data from UK infrastructure and networks. Maksim YAKUBETS was a central figure in the administration and leadership of Evil Corp and was responsible for managing and overseeing the group's malicious cyber activities. Additionally, Maksim YAKUBETS was involved in the development of Evil Corp's malware and ransomware strains. Evil Corp's malicious cyber activity involved a concerted effort to compromise UK health, government and public sector institutions, and commercial technology companies, for financial gain, which undermined or was intended to undermine the integrity, prosperity and security of the United Kingdom and its allies. (Gender): Male **Listed on:** 01/10/2024 **UK Sanctions List Date Designated:** 01/10/2024 **Last updated:** ~~01/10/2024~~ *08/10/2024* **Group ID:** 16583.

Office of Financial Sanctions Implementation

HM Treasury

08/10/2024