FINANCIAL SERVICES COMMISSION

19 November 2025

Financial Sanction Notice

Directions from Financial Services Commission

Please be informed that 1 entry has been amended under the Cyber financial sanctions regime.

On 19 November 2025, the Foreign, Commonwealth and Development Office updated the UK Sanctions List on Gov.Uk. This list provides details of those details designated under regulations made under the Sanctions Act.

1 entry has been amended under the Cyber financial sanctions regime and remains subject to an asset freeze.

The consolidated list of asset freeze targets has been updated to reflect these changes.

The notice will also be placed on our website at www.fscmontserrat.org (http://www.fscmontserrat.org) under the heading "Sanctions" for your future reference.

Please be guided accordingly.

FINANCIAL SERVICES COMMISSION

19 November 2025

Financial Sanction Notice

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. On 19 November 2025 the Foreign, Commonwealth and Development Office updated the UK Sanctions List on GOV.UK. This list provides details of those designated under regulations made under the Sanctions Act. A link to the UK Sanctions List can be found below.

3. Following the publication of the UK Sanctions List, information on the Consolidated List has been updated.

Notice summary

4. The following entry has been amended and is still subject to an asset freeze:

    - CHOSUN EXPO (Group ID: 13910

What <u>you</u> must do

5. 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.

6. 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.

7. Information regarding a suspected designated person, and funds or economic resources belonging to them, does not need to be disclosed to OFSI where it has previously been reported.

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

Ransomware and Sanctions

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

10. 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.

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

Further Information

12. 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.

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

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

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

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

Enquiries

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

Her Excellency, the Governor
The Governor's Office
#8 Farara Plaza
Brades, MSR 1110
E-Mail: michelle.webster@fcdo.gov.uk

ANNEX TO NOTICE

FINANCIAL SANCTIONS: CYBER

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

AMENDMENTS

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

Entity

1. ~~**CHOSUN EXPO (APT 38)**~~ ***CHOSUN EXPO***
a.k.a: (1) Chosen Expo (2) Korean Export Joint Venture **Address:** North Korea. **Other Information:** (UK Sanctions List Ref): CYB0004. (UK Statement of Reasons): ~~The Lazarus Group was responsible for relevant cyber activity that resulted in data interference which directly or indirectly caused, or is intended to cause, economic loss to, or prejudice to the commercial interests of, those affected by the activity through stealing money from Bangladesh Bank, attempting to steal money from Vietnam Tien Phong Bank and targeting the Polish Financial Conduct Authority information systems. Through the WannaCry attack they undermined the integrity of the United Kingdom through interfering with an information system so that it prevented the provision of essential healthcare services to the population~~. *Chosun Expo, a front company used by malicious cyber actors operating under the Reconnaissance General Bureau (RGB), has been responsible for, engaging in, providing support for, or promoting the commissions, planning or preparation of relevant cyber activity, including data interference and accessing information systems. Such activity that Chosun Expo is or has been involved in undermines, or is intended to undermine, the integrity, prosperity or security of the United Kingdom or a country other than the United Kingdom and directly or indirectly caused economic loss to, or prejudice to the commercial interests of, those affected by the activity*. (Type of entity): Company (Subsidiaries): Reconnaissance General Bureau **Listed on:** 31/07/2020 **UK Sanctions List Date Designated:** 31/12/2020 **Last Updated:** ~~31/12/2020~~ *19/11/2025* **Group ID:** 13910.

Financial Services Commission

19/11/2025