National Crime Agency

NECC

NATIONAL ECONOMIC CRIME CENTRE

jmlit

Joint Money Laundering Intelligence Taskforce

Office of Financial Sanctions Implementation
HM Treasury

Red ALERT

Exporting High Risk Goods

Date: December 2023
Reference: 0737-NECC

This Red Alert is issued by the National Economic Crime Centre (NECC), a multi-agency unit in the National Crime Agency (NCA), HM Treasury's Office of Financial Sanctions Implementation (OFSI) and the Foreign, Commonwealth & Development Office (FCDO), working in conjunction with law enforcement and financial sector partners as part of the Joint Money Laundering Intelligence Taskforce (JMLIT). The JMLIT is managed in the NECC and was established to ensure a more collaborative approach between law enforcement and the banking and wider private sector.

This Alert is devised with the aim of promoting awareness and bringing about preventative action. We recommend you use this Alert to complement existing knowledge and support ongoing improvements to your business processes and procedures.

Overview

The purpose of this Alert is to provide information to UK businesses on common techniques suspected to be in use to evade sanctions on the export of high-risk goods, which Russia is using on the battlefield in Ukraine.[1] The primary audience for this alert is the UK's financial sector, including banks, credit card operators, foreign exchange dealers and non-bank payment service providers. It may also be relevant to business sectors outside the regulated sector for anti-money laundering, in particular customs brokers, freight forwarders and other transportation and logistics providers.

This alert is issued by the JMLIT+ Financial Sanctions Circumvention Cell of the Money Laundering Public-Private Threat Group (ML PPTG), with representation from government, law enforcement and private industry.

What we would like you to do

The National Crime Agency (NCA) is a national law-enforcement agency which leads the UK's fight to cut serious and organised crime. The NCA Alerts process is the way in which we provide information to non-law enforcement bodies including the private sector to combat and disrupt serious crime. To help us to improve this service, we would welcome any feedback you have on both the Alert itself and the information provided to you. Please email all feedback to alerts@nca.gov.uk and include the reference **0737-NECC** in the subject line.

If you identify activity which may be indicative of the typology detailed in this report, and your business falls under the regulated sector, you may wish to make a Suspicious Activity Report [SAR]. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include **XXJMLXX** within the text and the reference **0737-NECC** for this alert. Further information and guidance is available at:

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports

For goods and associated services, if you discover that you have breached any of the trade prohibitions or licensing provisions, you should report the irregularity to HMRC (sometimes known as 'voluntary disclosure') as soon as possible. If the irregularity was found on an Export Control Joint Unit compliance audit, the compliance inspector will have informed HMRC and you are strongly advised to do the same. Guidance is available on how to make a voluntary disclosure here.

If you discover that you have breached any of the professional and business services trade prohibitions or licensing provisions, you should report the irregularity to the Department for Business and Trade (DBT) at servicestradebans@beis.gov.uk.

HM Treasury's Office of Financial Sanctions Implementation (OFSI) is the UK's competent authority for the implementation of financial sanctions. If you identify information that is indicative of either a frozen asset or of a breach of financial sanctions, such as dealing with frozen assets or funds involving a designated person, then you must report this to OFSI. Please email all such information to OFSI@hmtreasury.gov.uk.

[1] "High-risk goods" refers to Western items critical to Russian weapons systems and its military development. It includes, but is not exclusive to, dual-use goods.

For more information, please refer to https://www.gov.uk/government/publications/russia-sanctions-common-high-priority-items-list/russia-sanctions-common-high-priority-items-list

Information Report

In response to Russia's invasion of Ukraine, the UK and its partners have put in place an unprecedented package of sanctions aimed at cutting off funding and support for Russia's war machine, inflicting severe economic costs and showing solidarity with the Ukrainian people. The UK has prohibited all new investment into Russia and sanctioned over 1900 individuals and entities under the Russian Sanctions regime, including over 130 oligarchs with a combined net worth of over £140 billion in February 2022, and major Russian banks accounting for over 90% of Russia's banking sector. Over £20 billion of UK-Russia bilateral trade is now under full or partial sanctions. A price cap on Russian oil exports to third countries is further stifling Russia's efforts to fund and equip its military.

Earlier this year, G7 partners announced the Enforcement Coordination Mechanism to bolster compliance and enforcement of our measures and deny Russia the benefits that come with access to G7 economies including the access to advanced goods, technologies and services. The G7 called on third countries or other international actors to cease providing material support to Russia's war or face severe costs.

Direct trade between the UK and Russia has fallen to historic lows. However, Russia is exerting significant effort to procure sanctioned goods from other countries, including goods originating in the UK. Russia is deploying complex supply chains and alternative supply routes to acquire sanctioned products.

To address this, the UK, US, EU and Japan have developed a Common High Priority items list. The list, which will be updated when required, includes many items found on the battlefield in Ukraine, and includes integrated circuits, as well as other electrical and mechanical components. Items on this list are at high risk of being used in Russian sanctions circumvention efforts. UK businesses should conduct due diligence to ensure that the end destination of these products is not Russia. The UK government is also working with third countries to tackle the flow of these goods to Russia. The Department for Business and Trade published a notice for exporters to consider these risks and the role they play in the procurement cycle.

As well as working closely with third countries to highlight the risks of sanctions evasion, the UK and its partners have taken action to sanction entities - including in third countries - involved in supporting Russia's efforts to circumvent sanctions.

For example, on 8 August 2023 the UK took action to target Russia's defence systems by cutting off the Russian government's access to foreign military equipment. Among those sanctioned included two Turkey based businesses, TURKIK UNION and AZU INTERNATIONAL, for their role in exporting microelectronics to Russia that are essential for Russia's military activity in Ukraine, and Dubai-based AEROMOTUS UNMANNED AERIAL VEHICLES TRADING LLC, for its role in supplying drones and drone components to Russia.

On 8 November 2023, the UK also sanctioned LIMITED LIABILITY COMPANY TECHNOLOGICAL COMPANY FLY BRIDGE, a Russian company procuring dual-use goods for Russian electronics producers NPP ISTOK and ECITECH. On 6 December 2023, the UK announced sanctions against individuals and groups supplying and funding Putin's war machine. This included businesses in Belarus, China, Serbia, Turkey, the UAE and Uzbekistan, who continue to support Russia's illegal invasion of Ukraine.

HMRC, NCA, HMT, DBT and the FCDO will continue to work through established public-private partnerships to understand the exposure of UK businesses to the trade in goods critical to Russia's military industrial complex and to cut off this diversionary trade.

Indicators for the Financial Sector

The financial sector plays a critical role in the procurement cycle. The UK government encourages the financial sector, including banks, credit card operators, foreign exchange dealers and non-bank payment service providers, to ensure they are maintaining vigilance against global attempts to circumvent trade sanctions.

This includes taking steps to detect this activity and protect their business from Russian procurement activity by utilising data sources, screening, and monitoring capabilities. This can include drawing on transaction activity and customer attributes which may be indicative of the red flags below.

No single red flag is necessarily indicative of illicit or suspicious activity, all the surrounding facts and circumstances should be considered before determining whether a specific transaction or customer is suspicious or associated with potential sanctions evasion.

1. Transactions related to payments for goods on the Common High Priority list, from a company incorporated after 24 February 2022 and based in known diversionary destinations.
2. A customer who lacks or refuses to provide details on banks, shippers, or third parties, including about end users, intended end-use, or company ownership.
3. Transactions involving smaller value payments, all from the same end user's foreign bank account, to multiple, similar suppliers of Common High Priority list items.
4. A customer that significantly overpays for a Common High Priority list item, compared to known market prices.
5. Purchases under a letter of credit that are consigned to the issuing bank, not to the actual end user. In addition, supporting documents, such as a commercial invoice, do not list the actual end-user.
6. Transactions involving entities with little to no web presence, such as a website or a domain-based email account.
7. Transactions involving customers with phone numbers with country codes that do not match the destination country.
8. The item or service (commodity, software, service or technology) does not fit the purchaser's line of business.
9. The customer's name or its address is similar to one of the parties on the OFSI consolidated list.
10. Transactions involve a purported civil end-user, but research indicates customers with counterparties with connections with the military, such as an address that is a military facility or is co-located with military facilities in a country of concern.
11. Transactions involving companies that are physically co-located, or have shared ownership, with an entity on the OFSI consolidated list.
12. Transactions that use open accounts/open lines of credit when the payment services are conducted in conjunction with known diversionary destinations.

13. Transactions involving a last-minute change in payment routing that was previously scheduled from a country of concern, but now routed through a different country or company.

14. Transactions involving payments being made from entities located at known transhipment points or involve atypical shipping routes to reach a destination.

Data Protection Act

The NCA reminds you of your legal obligations in respect of the management of this information, including under the Data Protection Act 2018.

Article 5(1) requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for a specified, explicit and legitimate purpose and not further processed in a manner that's incompatible with these purposes;
3. Adequate, relevant and limited to what's necessary in relation to the purpose for which they are processed;
4. Accurate and where necessary kept up to date;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data.

Suspicious Activity Reporting [SARs]

If you know or suspect that there has been money laundering or terrorist financing activity (including as a result of information provided to you by the NCA) and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the NCA under Part 7 Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference **0737-NECC** within the text. This reference is specific to the Alerts process; where appropriate, we would ask that this is used *in addition* to the ongoing use of the Glossary of Terms. Guidance on making suspicious activity reports is available at www.nationalcrimeagency.gov.uk.

Disclaimer

While every effort is made to ensure the accuracy of any information or other material contained in or associated with this document, it is provided on the basis that the NCA and its staff, either individually or collectively, accept no responsibility for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any such information or material.

Any use by you or by any third party of information or other material contained in or associated with this document signifies agreement by you or them to these conditions.

Protecting this document

This document uses the United Kingdom's Government Security Classification System (GSCS) and has been graded as **OFFICIAL**. There are no specific requirements for storage and it can be considered safe for wide distribution within your organisation and for use in staff training or awareness programmes. However, unless otherwise specified, this information is not intended for general public dissemination and should not be included on public facing websites, external mailing lists, social media or other outlets routinely used by you to deliver information to the public without the prior and specific permission of the NCA Alerts team. We therefore request that you risk manage any onward dissemination in a considered way. This document should be disposed of by cross-cut shredder, pulping or incineration.

Alert Markings

NCA Alerts are marked either Red or Amber. This is designed to indicate the urgency of the warning. Red may indicate a more immediate or specific threat, whilst those marked Amber will provide more general information that may complement existing knowledge.

NCA Alerts Team

Recognising that the private sector is often the victim of serious organised crime and is engaged in its own efforts to prevent, deter and frustrate criminal activity, the NCA seeks to forge new relationships with business and commerce that will be to our mutual benefit – and to the criminals' cost. By issuing Alerts that warn of criminal dangers and threats, NCA seeks to arm the private sector with information and advice it can use to protect itself and the public. For further information about this NCA Alert, please contact the NCA Alerts team by email alerts@nca.gov.uk. For more information about the National Crime Agency go to www.nationalcrimeagency.gov.uk.

Protecting the Public – Providing information back to the NCA

Section 7(1) of the Crime and Courts Act 2013 allows you to disclose information to the NCA, provided the disclosure is made for the purposes of discharging the NCA's functions of combating serious, organised and other kinds of crime. The disclosure of such information to the NCA will not breach any obligation of confidence you may owe to a third party or any other restrictions (however imposed) on the disclosure of this information. The disclosure of personal information about a living individual by you to the NCA must still comply with the provisions of the Data Protection Act 2018 (DPA). However, you may be satisfied that the disclosure by you of such personal information to the NCA in order to assist the NCA in carrying out its functions may be permitted by Schedule 2, Part 1 of the DPA 2018. This allows a data controller to be exempt (by means of a restriction or adaption) from provisions of the GDPR, if the personal data is processed for the following purposes:

> *a) the prevention or detection of crime,*
>
> *b) the apprehension or prosecution of offenders, or*
>
> *c) the assessment or collection of a tax or duty or an imposition of a similar nature,*
>
> *to the extent that the application of those provisions of the GDPR would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).*
>
> (DPA 2018, Schedule 2, Part 1).

Any Section 7(1) information should be submitted to alerts@nca.gov.uk. The NCA's Information Charter is published on our external website at www.nca.gov.uk.

Handling advice – Legal information

This information is supplied by the UK's NCA under Section 7(4) of the Crime and Courts Act 2013. It is exempt from disclosure under the Freedom of Information Act 2000. It may be subject to exemptions under other UK legislation. Except where permitted by any accompanying handling instructions, this information must not be further disclosed without the NCA's prior consent, pursuant to schedule 7, Part 3, of the Crime and Courts Act 2013.

This report may contain 'Sensitive Material' as defined in the Attorney General's guidelines for the disclosure of 'Unused Material' to the defence. Any sensitive material contained in this report may be subject to the concept of Public Interest Immunity. No part of this report should be disclosed to the defence without prior consultation with the originator.

Requests for further disclosure which are not permitted by any handling instructions or handling code must be referred to the NCA originator from whom you received this information, save that requests for disclosure to third parties under the provisions of the Data Protection Act 2018 or the Freedom of Information Act 2000 and equivalent legislation must be referred to the NCA's Statutory Disclosure Team by e-mail on statutorydisclosureteam@nca.gov.uk.